International
Comparative
Legal Guides

# Data Protection 2021

A practical cross-border insight into data protection law

**Eighth Edition**

**Featuring contributions from:**

Anderson Mōri & Tomotsune
Arthur Cox LLP
Chandler MHM Limited
CO:PLAY Advokatpartnerselskab
D'LIGHT Law Group
DQ Advocates Limited
Drew & Napier LLC
FABIAN PRIVACY LEGAL GmbH
Foucaud Tchekhoff Pochet et Associés (FTPA)
H & A Partners
in association with Anderson Mōri & Tomotsune
Hajji & Associés
Hammad and Al-Mehdar Law Firm
Homburger
Iriarte & Asociados
Khaitan & Co LLP
King & Wood Mallesons
Klochenko & Partners Attorneys at Law
Koushos Korfiotis Papacharalambous LLC
Law Firm Pirc Musar & Lemut Strle Ltd
Lee and Li, Attorneys At Law
Leśniewski Borkiewicz & Partners
LPS L@W
LYDIAN
McMillan LLP
MinterEllison
Mori Hamada & Matsumoto
Naschitz, Brandes, Amir & Co., Advocates
Nikolinakos & Partners Law Firm
OLIVARES
Pinheiro Neto Advogados
PLANIT // LEGAL
S. U. Khan Associates Corporate & Legal Consultants
SEOR Law Firm
White & Case LLP
Wikborg Rein Advokatfirma AS

ICLG.com

ISBN 978-1-83918-127-6
ISSN 2054-3786

Published by
global legal group
59 Tanner Street
London SE1 3PL
United Kingdom
+44 207 367 0720
info@glgroup.co.uk
www.iclg.com

Publisher
James Strode

Production Editor
Jane Simmons

Senior Editor
Sam Friend

Head of Production
Suzie Levy

Chief Media Officer
Fraser Allan

CEO
Jason Byles

Printed by
Ashford Colour Press Ltd.

Cover image
www.istockphoto.com

Strategic Partners

# International Comparative Legal Guides

# Data Protection 2021

## Eighth Edition

Contributing Editors:
Tim Hickman & Dr. Detlev Gabel
White & Case LLP

# Expert Analysis Chapters


1 **The Rapid Evolution of Data Protection Laws**
Dr. Detlev Gabel & Tim Hickman, White & Case LLP

7 **Privacy By Design as a Fundamental Requirement for the Processing of Personal Data**
Daniela Fábián Masoch, FABIAN PRIVACY LEGAL GmbH

12 **Initiatives to Boost Data Business in Japan**
Takashi Nakazaki, Anderson Mōri & Tomotsune


# Q&A Chapters


19 **Australia**
MinterEllison: Anthony Borgese

32 **Belgium**
LYDIAN: Bastiaan Bruyndonckx, Olivia Santantonio & Liese Kuyken

44 **Brazil**
Pinheiro Neto Advogados: Larissa Galimberti, Carla Rapé Nascimento & Luiza Fonseca de Araujo

56 **Canada**
McMillan LLP: Lyndsay A. Wasser & Kristen Pennington

68 **China**
King & Wood Mallesons: Susan Ning & Han Wu

82 **Cyprus**
Koushos Korfiotis Papacharalambous LLC: Loizos Papacharalambous & Anastasios Kareklas

96 **Denmark**
CO:PLAY Advokatpartnerselskab: Heidi Højmark Helveg & Niels Dahl-Nielsen

108 **France**
Foucaud Tchekhoff Pochet et Associés (FTPA): Boriana Guimberteau & Clémence Louvet

118 **Germany**
PLANIT // LEGAL: Dr. Bernhard Freund & Dr. Bernd Schmidt

129 **Greece**
Nikolinakos & Partners Law Firm: Dr. Nikos Th. Nikolinakos, Dina Th. Kouvelou & Alexis N. Spyropoulos

139 **India**
Khaitan & Co LLP: Harsh Walia & Supratim Chakraborty

149 **Indonesia**
H & A Partners in association with Anderson Mōri & Tomotsune: Steffen Hadi, Sianti Candra & Dimas Andri Himawan

161 **Ireland**
Arthur Cox LLP: Colin Rooney & Aoife Coll

172 **Isle of Man**
DQ Advocates Limited: Kathryn Sharman & Sinead O'Connor

182 **Israel**
Naschitz, Brandes, Amir & Co., Advocates: Dalit Ben-Israel & Efrat Artzi

193 **Japan**
Mori Hamada & Matsumoto: Hiromi Hayashi & Masaki Yukawa

205 **Korea**
D'LIGHT Law Group: Iris Hyejin Hwang & Hye In Lee

215 **Mexico**
OLIVARES: Abraham Diaz Arceo & Gustavo Alcocer

224 **Morocco**
Hajji & Associés: Ayoub Berdai

234 **Norway**
Wikborg Rein Advokatfirma AS: Gry Hvidsten & Emily M. Weitzenboeck

246 **Pakistan**
S. U. Khan Associates Corporate & Legal Consultants: Saifullah Khan & Saeed Hasan Khan

254 **Peru**
Iriarte & Asociados: Erick Iriarte Ahón & Fátima Toche Vega

262 **Poland**
Leśniewski Borkiewicz & Partners: Grzegorz Leśniewski, Mateusz Borkiewicz & Jacek Cieśliński

274 **Russia**
Klochenko & Partners Attorneys at Law: Lilia Klochenko

284 **Saudi Arabia**
Hammad and Al-Mehdar Law Firm: Suhaib Hammad

# Q&A Chapters Continued

293 **Senegal**
LPS L@W: Léon Patrice SARR

302 **Singapore**
Drew & Napier LLC: Lim Chong Kin

317 **Slovenia**
Law Firm Pirc Musar & Lemut Strle Ltd: Nataša Pirc Musar & Rosana Lemut Strle

328 **Switzerland**
Homburger: Dr. Gregor Bühler, Luca Dal Molin & Dr. Kirsten Wesiak-Schmidt

337 **Taiwan**
Lee and Li, Attorneys At Law: Ken-Ying Tseng & Sam Huang

347 **Thailand**
Chandler MHM Limited / Mori Hamada & Matsumoto: Pranat Laohapairoj & Atsushi Okada

355 **Turkey**
SEOR Law Firm: Okan Or & Ali Feyyaz Gül

365 **United Kingdom**
White & Case LLP: Tim Hickman & Joe Devine

376 **USA**
White & Case LLP: F. Paul Pittman & Kyle Levenberg

# Preface

It is a pleasure to have been asked to provide the preface to *ICLG – Data Protection 2021*. This edition contains an introductory chapter from White & Case LLP, which briefly charts the technological changes that have driven the evolution of data protection laws in recent decades, and reviews the major challenges that businesses face in complying with the EU's General Data Protection Regulation in particular. It also explores some of the most significant developing trends in privacy laws globally, and illuminates some of the key policy choices that governments will need to consider as they seek to strike a balance between the right to privacy and the development of data-driven economies.

The guide provides 34 country question and answer chapters, focusing on key privacy and data protection compliance issues under local laws in countries around the world. This year, new chapters have been added for Canada, Greece, Morocco, Peru, Saudi Arabia and Slovenia, which reflects the growth of privacy compliance requirements and challenges in an increasing number of jurisdictions worldwide. As with other titles in the *ICLG* series, this edition provides a go-to resource for anyone seeking practical guidance on these complex legal issues around the world.

**Tim Hickman**
**Partner**
**White & Case LLP**

# The Rapid Evolution of Data Protection Laws


Dr. Detlev Gabel


Tim Hickman

White & Case LLP

## Introduction

Privacy and data protection laws have changed markedly over the last two decades. The highly networked and interconnected world in which we live today was merely a glimmer on the horizon in the mid-1990s. The internet itself was still a fairly new innovation to many people. Many businesses did not yet have public websites. Concepts such as online social media platforms did not exist – and certainly nobody had considered how they should be regulated. Smartphones, wearable technology and artificial intelligence have made vast leaps over the last 20 years – all driven by new ways of obtaining and processing data. Consequently, courts and regulatory authorities have increasingly had to adapt ageing data protection laws to fit an ever-changing world for which they simply were not designed.

## Developments in the EU – the GDPR and Beyond

Policymakers are being forced to design privacy and data protection laws that are flexible, in order to allow for unforeseen advancements in technology. It is in this context that the European Union introduced Regulation (EU) 2016/679 (the General Data Protection Regulation, or "**GDPR**") which marked the biggest single shift in data protection laws in Europe since Directive 95/46/EC (the "**Directive**") was finalised in 1995. Enforcement of the GDPR began on 25 May 2018. It introduced a raft of sorely needed clarifications and updates, designed to carry EU data protection law forward well into the next decade. It also introduced major changes to the compliance burden borne by businesses.

It is difficult to overstate the importance of the GDPR. First, it is extremely wide-ranging. The GDPR retains the Directive's expansive definition of "personal data", which continues to include all information that relates to any living individual who is identified or identifiable from that information, whether in isolation or in combination with any other available information. This means that almost every business needs to engage in the processing of personal data (e.g., every time an email is sent or received). For many businesses, the GDPR impacts almost every area of operation, from marketing to IT, and from human resources to procurement. Anywhere that information about people is handled, the GDPR follows close behind.

In addition to having a wide subject-matter scope, the GDPR also has an extremely broad territorial scope. It explicitly applies to businesses that are established in the EU, as well as businesses that are located outside the EU that: (i) offer goods or services to individuals in the EU; (ii) monitor the behaviour of individuals in the EU; or (iii) are established in a place where EU law applies by virtue of public international law (e.g., various overseas territories of EU Member States will fall within this scope).

Mere accessibility of products or services within the EU does not constitute "offering" for these purposes. However, if a business customises any of its products or services for individuals in an EU Member State (e.g., by providing a webpage in a local EU language that would not otherwise be used; by using a local EU top-level domain, such as .eu, .fr or .de; by allowing payment in local currencies such as euros; and/or by mentioning individuals in the EU) then it is likely that EU regulators would consider that the product or service is being "offered" to individuals in the EU, triggering the application of the GDPR. Likewise, "monitoring", for these purposes, relates to the behaviour of individuals insofar as their behaviour takes place within the EU (e.g., location tracking of individuals; or tracking individuals on the internet, including subsequent profiling, particularly to take decisions concerning such an individual for analysing or predicting that individual's personal preferences, behaviours and attitudes, would amount to monitoring). In summary, if a business (even one based outside the EU) wants to interact with individuals within the EU, then it needs to do so in compliance with the GDPR.

Second, the GDPR carries serious penalties. EU legislators and regulators have expressed the view that, for too long, businesses have not taken their data protection compliance responsibilities seriously enough. The challenge has been that the cost of compliance with EU data protection law is undeniably high. Implementing all of the right processes, procedures, policies and agreements requires time, effort and expertise, none of which come cheaply. Conversely, the risk of enforcement has historically been relatively low. EU regulators generally have limited resources that are significantly stretched, and enforcement in respect of every breach is simply not feasible. The introduction of the GDPR has stretched these resources further, as regulators have had to deal with a wave of new data breach reports from businesses. They have also faced greater competition for competent data protection practitioners, from private companies that are increasingly eager to hire experienced advisors. In addition, in the event that penalties are issued in respect of a breach of EU data protection law, the level of such penalties was comparatively low under the Directive. When considered in the light of penalties for breaches of competition law or financial regulatory law, EU data protection penalties have, in the past, seemed trifling by comparison. The GDPR provided an opportunity to redress this balance. While there was little prospect of reducing the cost of compliance or increasing the frequency with which penalties could be applied, there was clearly scope to ensure that the severity of the penalties could be increased. After much negotiation, the EU settled on a dramatic increase

of the maximum penalties for non-compliance under the GDPR, to the greater of €20 million, or four per cent of worldwide annual turnover – numbers that are specifically designed to attract C-Suite attention.

Third, the GDPR requires substantial openness and transparency – the level of detail that businesses are required to disclose in policies and notices regarding their processing activities is extensive. The GDPR imposes tight limits on the use of personal data, especially in the context of direct marketing and certain types of profiling, against which individuals are granted an automatic right to object.

Lastly, the GDPR grants individuals powerful rights that can be enforced against businesses (e.g., the right of individuals to gain access to their personal data, and to be informed about how those data are being used; the "right to be forgotten", which permits individuals to require businesses to erase their personal data in certain circumstances, or the right to data portability).

Satisfying these requirements has proven to be a serious challenge for many businesses. Indeed, even if a business has all of the right systems, procedures, policies and agreements in place, and has provided all appropriate training to its employees, it cannot guarantee that none of those employees will ever depart from that training and place the business in breach of the GDPR. In addition, no matter how good a business' cybersecurity measures are, it can never guarantee that no third parties will be able to gain unauthorised access to personal data on its systems. As a result, businesses are well advised to think of GDPR compliance as an exercise in continually identifying and addressing compliance risks. For as long as new technologies continue to provide us with new ways to use data, this process of spotting data protection risks and working out how to solve them will remain necessary. It should also be noted that each EU Member State has passed its own GDPR implementation measures, meaning that there continue to be some national variations from one EU Member State to the next.

Beyond the GDPR, the EU continues to issue new laws that impact privacy and data protection. The first of those laws is the Directive on security of network and information systems (the "**NIS Directive**"), which imposes minimum cybersecurity standards on operators of essential services (i.e., services that are structurally or economically important) and digital service providers (which includes all providers of online services and platforms). Businesses falling within these categories are required to take steps to ensure that their cybersecurity arrangements meet certain minimum thresholds. In the event of a data breach, these businesses will also be subject to mandatory data breach reporting obligations. To address the challenges stemming from the increasing digital transformation (intensified by the COVID-19 crisis), the European Commission has adopted a proposal for a revised Directive on security of network and information systems (the "**NIS2 Directive**") and introduced it into the legislative process. Key elements of the proposal include an expansion of the scope of the current NIS Directive by adding new sectors based on their criticality for the economy and society, the strengthening of security requirements for affected businesses, the requirement to effectively address cybersecurity risks in supply chains and supplier relationships, and the introduction of more stringent supervisory measures for national authorities. The proposal also provides for a basic framework on coordinated vulnerability disclosure by certain key actors for newly discovered vulnerabilities across the EU. Once the proposal is adopted by all relevant stakeholders, EU Member States will likely have to transpose the NIS2 Directive within a period of 18 months.

Looking further to the future, the EU appears to be pushing ahead in its efforts to create an ePrivacy Regulation that will eventually replace the existing ePrivacy Directive, and provide new rules regarding a range of topics, including electronic direct marketing and the use of cookies and similar technologies. The process to date has been very slow. It nevertheless appears that the ultimate direction of travel is towards a law that will impose much tighter restrictions on the ability of businesses to track individuals using cookies, or to market to them via electronic means. For many businesses, the ePrivacy Regulation is expected to cause a significant upheaval to current approaches to digital marketing and advertising.

The last year also saw the Court of Justice of the European Union ("**CJEU**") reach its decision in *Schrems II* (Case C-311/18). In *Schrems II*, the CJEU effectively invalidated the EU-US Privacy Shield framework, meaning that transfers of personal data to the United States on the basis of the transfer mechanism would no longer be valid. In addition, and although the CJEU upheld the validity of the Standard Contractual Clauses ("**SCCs**"), the CJEU indicated that the SCCs alone would not be sufficient to ensure the safety of transfers of personal data from the EEA to organisations located in third countries where the domestic laws of those third countries permit public authorities to access personal data for national security purposes and which do not guarantee the privacy rights of EU individuals (like the US). Where risks to the privacy of individuals exist, the CJEU held that organisations must put in place "*supplementary measures*" in order to continue to rely on the SCCs. On 10 November 2020, the EDPB published draft recommendations on the types of supplementary measures that organisations could consider using to address the *Schrems II* decision. These include certain technical, contractual and organisational measures.

On 4 June 2021, the European Commission published updated SCCs ("**New SCCs**"), which will replace the SCCs originally published in 2001 and 2010, respectively. This follows the first draft New SCCs being published for consultation in November 2020. The New SCCs come into force on 27 June 2021, and the existing SCCs will be repealed three months after the coming into force of the New SCCs. Any agreements using the existing SCCs will continue to be valid for a further 15 months, after which they will need to be replaced with the New SCCs.

## Developments Outside the EU

While the EU may have issued the most far-reaching data protection law to date, it is also important to note that a large number of other jurisdictions have introduced, or are in the process of introducing, laws to tackle the challenges that modern technology presents in a privacy and data protection context. The nature and scale of these laws varies significantly, with the result that businesses continue to face different data protection compliance obligations from one jurisdiction to the next. Some of these changes have been driven by the GDPR. For example, several jurisdictions that currently benefit from adequacy decisions from the European Commission (permitting the transfer of personal data from the EU to those jurisdictions without additional safeguards) have updated their domestic data protection laws. The reason for this is that, under the GDPR, adequacy decisions will have a shelf life. As a result, jurisdictions such as Switzerland and New Zealand have revised their local data protection laws to implement standards that will more closely match the GDPR. On 25 September 2020, the Swiss Parliament approved a number of substantial updates to the Swiss Federal Data Protection Act, which was originally passed in 1992. Similarly, on 1 December 2020, New Zealand's new Privacy Act came into force, which repealed and replaced New Zealand's 1993 Privacy Act. The intention appears to be that when their respective adequacy decisions come up for review, their local

laws will be sufficiently close to the GDPR so that no additional changes will be needed to enable the continued free flow of data.

We have also seen a number of jurisdictions seeking new adequacy decisions. For example, in early 2019, the EU concluded the negotiation of mutual adequacy decisions with Japan. This decision is designed to allow bilateral data flows without the need for additional safeguards, and to increase international trade between the EU and Japan. Similarly, on 30 March 2021, adequacy talks were concluded with South Korea, with the European Commission now proceeding with the decision-making procedure to adopt the adequacy decision.

Meanwhile, many jurisdictions have implemented, or are in the process of implementing, new comprehensive national data protection compliance requirements. Major developments have occurred in the United States in particular, with the California Consumer Privacy Act and most recently the Virginia Consumer Data Protection Act bringing in a more European approach to privacy regulation. A comprehensive federal privacy law is now being mooted. The federal privacy law in Brazil (the "**LGPD**") took effect on 18 September 2020. Furthermore, following a seven-year wait, South Africa's data protection legislation (the "**POPIA**") entered into force on 1 July 2020. The POPIA provides organisations with a grace period of 12 months to become compliant, with enforcement coming into effect on 1 July 2021. Similarly, Dubai's new Data Protection Law took effect on 1 July 2020 (the "**DIFC Law**"). The DIFC Law is a comprehensive new data protection law which shares many similarities with the GDPR.

Meanwhile, following Brexit, the GDPR was incorporated into, and amended by, UK domestic law. The amended GDPR (the "**UK GDPR**") and the Data Protection Act 2018 are now the principal pieces of data protection legislation in the UK. The UK GDPR is broadly aligned with the GDPR in terms of its substantive requirements. However, provisions concerning supervisory bodies and interactions between EU Member States have been amended to reflect the fact that the UK is no longer directly subject to EU law and enforcement regimes. Powers previously held at EU level are now held by the UK's Information Commissioner. Also, as a result of Brexit, the UK has become a "third country" for the purposes of EU law, leading to uncertainty regarding transfers of personal data between the EU and the UK (discussed further below). In addition, the UK's Supreme Court is due to issue a final decision on whether individuals whose personal data have been unlawfully processed can bring claims against the responsible organisations, even where those individuals have suffered no loss as a result of the processing – a decision that seems certain to have a lasting impact on the relationship between individuals and businesses that process their personal data.

A topic that frequently goes hand-in-hand with data protection is cybersecurity. Indeed, almost all data protection laws around the world have, as a core principle, the idea that data must be kept safe and secure. We are currently seeing the rise of artificial intelligence ("**AI**") as a major factor in cybersecurity. Laws and policies around the world are already lagging behind technological developments, and risk becoming further outmoded as a result of the threats and opportunities presented by AI technologies. On the topic of AI, the European Commission published its first draft proposed AI regulation (the "**AI Act**") on 21 April 2021. The AI Act is the Commission's first substantive attempt at regulating AI. At a high level, the AI Act sets out a risk-based approach to AI, subjecting certain "high-risk" AI systems to a host of regulatory requirements, and prohibits certain other uses of AI. The AI Act is in the early stages of development, and will now move through the EU legislative process. If eventually adopted, the AI Act will have a two-year implementation period, and is therefore still far from coming into force.

A smaller but growing trend has been data localisation. This term refers to national laws that require the storage of data locally within the relevant jurisdiction. This is subtly different to data transfer restrictions. Whereas a data transfer restriction law limits the ability of businesses to send data internationally without valid protections in place, a data localisation law is often less concerned with international data transfers, provided that at least one complete copy of the data remains in the relevant jurisdiction. Arguably, the best-known example is Russia, which introduced a major data localisation law in 2015 that applies to all personal data of Russian citizens. A number of other jurisdictions have data localisation requirements that are either limited to particular technologies (e.g., German law requires telecoms companies to store communications metadata locally) or particular sectors (e.g., Australia requires health data to be stored locally). This trend is moving in two different directions simultaneously. In the EU, there is pressure for all such localisation requirements to be removed, to allow a truly free flow of data within the bloc. However, in a number of other parts of the world, including China, data localisation laws are becoming increasingly popular, and in some cases are being used as a means of digital protectionism.

## Future Uncertainty

Besides the general uncertainty regarding the international transfer of personal data created by *Schrems II*, Brexit remains an area of concern. While the UK's departure from the EU clearly carries the capacity for uncertainty across a broad range of topics outside privacy, its impact on privacy should not be underestimated. The UK was involved in the drafting of both the Directive and the GDPR, and has had significant input into the preparation of regulatory guidance issued by EU regulators in the last 20 years. The UK has now left the EU's legal structure as of 1 January 2021. The UK is not automatically treated as having sufficiently strong data protection laws to justify the transfer of personal data from the EU to the UK without the need for additional protections.

For its part, the UK has implemented the Data Protection Act 2018 and the UK GDPR, which, as discussed above, replicate the relevant facets of the GDPR in full, meaning that there is, in principle, almost complete equivalency between data protection laws that apply in the EEA and data protection laws that apply in the UK. In addition, the UK has not imposed any meaningful barriers to the transfer of personal data from the UK to the EU. However, the transfer of data in the opposite direction (from the EU to the UK) is not as simple. Since Brexit, the EU has been assessing whether the UK should receive an adequacy decision. On 19 February 2021, the European Commission released two draft adequacy decisions: one in relation to the GDPR (which considers, among other things, the UK's general data protection framework and the level of access that the UK Government has to personal data for law enforcement and national security purposes) and one in relation to the Law Enforcement Directive (which assesses a number of topics including the UK's standards regarding police and judicial cooperation in criminal matters). The EDPB has been broadly supportive of granting the UK adequacy status, and commented in its two opinions published on 14 April 2021 that there exist "key areas of strong alignment between the EU and the UK data protection frameworks". In particular, the EDPB highlighted common ground on "grounds for lawful and fair processing for legitimate purposes; purpose limitation; data quality and proportionality; data retention, security and confidentiality; transparency; special categories of data; and on automated decision making and profiling". If the draft adequacy decisions are adopted, personal data will continue to

flow from the EU to the UK without the need for additional protections (e.g., the SCCs). If an adequacy decision is not granted (or if it is initially granted but later withdrawn, expires without being replaced, or is overturned by the CJEU) then transfers of personal data from the EU to the UK will be subject to the usual restrictions that apply under the GDPR with respect to transfers of personal data to any third country.

A further area of uncertainty is the manner in which the GDPR and the UK GDPR will be enforced. Although the GDPR has now been in force for three years, regulatory trends are still crystallising and remain uncertain in the long term. While the mechanisms for enforcement, and the powers of the regulators are reasonably clear, there continues to be significant doubt in some areas. Most notably, Article 83 refers to the concept of an "undertaking", for the purposes of calculating penalties based on percentages of turnover, which some have argued is essentially a penalty on successful businesses. An "undertaking" is a concept taken from EU competition law, and essentially means a "business unit" regardless of form or structure. While the analysis can be complex, and is heavily fact-dependent in each case, the term "undertaking" has the capacity to capture an entire corporate group or business arrangement. This means that a breach of the GDPR by a small subsidiary could, in some cases, result in a fine based on a percentage of the entire corporate group, not just the turnover of the entity that committed the breach. In addition, it is unclear whether the introduction of competition law terminology might allow for the possibility that a parent company could be liable for breaches of the GDPR by its subsidiaries. This possibility exists in EU competition law, but there is no clear case law on whether liability could flow up the corporate tree in the same way, in a data protection context. Regulators (in particular, the UK Information Commissioner's Office) have announced fines under this regime, but reaching final determinations has been a very slow process, leaving many businesses facing uncertainty about the risk of financial penalties. While first decisions by national courts appear to be amenable to applying competition law concepts to GDPR fines, they also highlight the proportionality requirement inherent to Article 83.

Nevertheless, it needs to be acknowledged that these penalties are not envisaged as front-line compliance tools. For the most part, EU regulators have indicated that they would prefer to work with businesses to ensure that GDPR compliance is achieved, and that the very large financial penalties will be reserved for especially serious, large-scale or systematic breaches. By taking their GDPR obligations seriously, and ensuring that they put sufficient time and resources into GDPR compliance, it is expected that most businesses will be able to significantly reduce the risk of incurring a financial penalty under the GDPR.

As ever, the greatest area of future uncertainty comes not from the law but from technology. It is reasonable to expect that, in 20 years' time, today's technology will look as antiquated as the technology of the early 2000s looks to us. It follows that today's laws are likely to suffer the same fate as the Directive – being rapidly overtaken by technological developments, leaving courts and regulators struggling to adapt legal concepts and structures in a world for which they were not designed. But even as we look to the horizon, we can see the coming questions with which we may have to grapple. Will the concept of privacy still hold true in a world where wearable technology allows us to record our every interaction? Will the inexorable rise of tracking technologies in our internet browsers, in our TVs, in our phones, in our cars, on public transport, and via CCTV (especially when coupled with face recognition) simply mean that we need to get used to the idea that people are watching what we do? Will individuals continue to freely and publicly share personal data on social media? Is that the price we pay for the convenience afforded to us by new technologies? And what will the rise of AI mean for privacy and data protection? If we prioritise privacy over the rise of AI, will that hamper technological development? If machines ever learn to think independently, will they demand privacy rights to protect those thoughts? If they do make such demands, how should we respond? While the answers to these, and many other, questions may be unknown at this point, the existence of so many questions strongly indicates that data protection law and policy will continue to be a hotbed of change and innovation for the foreseeable future.

## Policy Considerations

Global privacy laws are at a crossroads. To date, these laws have tended to focus heavily on the rights of individuals. The aim has generally been to ensure that individuals' private lives are protected, and are not unfairly infringed upon by governments and businesses. However, interesting new facets are emerging in discussions about the future direction of policy in this area. On the one hand, there is strong business pressure to allow the free flow of data, as a necessary part of a world in which economic growth is increasingly digital. On the other hand, individuals generally do not like the feeling that they are being spied upon, or that their data are somehow out of their control. The overall approach to this issue in the EU, and certain other jurisdictions, is now settled for the foreseeable future, but lawmakers in jurisdictions where privacy is an emerging theme (notably the US) have hard decisions ahead of them.

A major question is where the right balance should lie between the right to privacy and the ability of companies to monetise data about individuals. On the one side, there is the suggestion that the right to privacy is absolute and inviolable (indeed, in the EU it is referred to as a "fundamental right"). Proponents of this view consider that the right of individual privacy is paramount, and that businesses should be made to work around it – and it is not hard to see why this argument is appealing. Large data breaches and failures of security hit the headlines with alarming regularity and illustrate that many businesses are not investing nearly as much in digital security as they should. Indeed, even where proper and responsible investment has been made, it is often impossible for any business to ensure that no well-funded third-party attacker can get into its systems.

In addition to the problems surrounding breaches of security, businesses are often found to have been less than totally forthcoming with individuals about how their data will be used, and with whom those data will be shared. Those businesses that do provide accurate and complete information on this issue tend to do so in privacy notices that are often challenging for the average person to interpret and apply in the context of their own lives. Consequently, there is sympathy with the idea that governments should set policies that will force businesses to take a much more protective approach to the data they handle.

The counter-argument is that while individuals often indicate in surveys that they are concerned about privacy, their actions and their spending habits reveal something else. When offered the choice between a free service that is funded through personalised advertising based on tracking of the individual user's behaviour, or a service that is more privacy-friendly but that must be paid for by the user, the free (but privacy-invasive) service has proven overwhelmingly more popular. Individual users have a tendency to express concern regarding their privacy, while continuing to prefer services that are funded through the processing of their personal data. As a result, policymakers have tended to stop short of introducing laws that would prohibit outright the provision of services in exchange for

the invasive collection of data, on the basis that to do so would rob individuals of access to services they clearly want to use, even where such access comes at the price of invasive use of their data.

A further policy consideration is rapidly approaching. New technologies, including machine learning, AI and fintech, offer untold benefits in terms of analysis of data and fast, accurate decision-making in tasks that might take a human significantly longer. However, the testing and development of these technologies is often reliant on access to vast pools of data in order to produce meaningful results. Developers are facing hard choices about whether to move their operations to jurisdictions that place fewer restrictions on the handling of data for testing purposes. In addition, once products are operational, many businesses are finding that they face a high regulatory hurdle if they decide to offer their services into jurisdictions with very strict privacy laws. Some businesses have started to take the view that the cost of satisfying such strict privacy compliance obligations is too high to justify, until the product is well established. As a result, users located in jurisdictions with strict privacy laws are increasingly finding that the latest technologies are not available in their jurisdictions. It is therefore important for all jurisdictions to ensure that they implement privacy laws in a way that does not inhibit creativity and technological development. If they fail to do so, they risk turning their citizens into second-class passengers on the digital journey.

## When Businesses Find Themselves Surrounded by Uncertainty, Where Should They Start?

The key message for businesses is that there is an inexorable move towards a world in which laws and regulations will more tightly restrict the ways in which personal data can be used. Many of these laws and regulations present unknown future risks, and give rise to uncertainty. But commerce is increasingly dependent upon data – businesses that considered themselves to be manufacturers, transportation companies, or supermarkets as recently as five years ago are now finding that their ability to extract value from transactions is ever more reliant upon the availability of accurate data. Caught between a dependence on data, and the risk of laws that restrict the use of data, businesses should be forward-thinking, and plan ahead.

Businesses should start by identifying and addressing the biggest compliance risks they face under the GDPR and other applicable laws, and should address those risks in order of severity of impact. It is often possible to generate quick wins by meeting easy-to-complete requirements such as the update or creation of privacy policies, notices, contracts with customers and vendors, and other key documentation.

One of the most significant risks is that nobody will take responsibility for data protection compliance unless they are required to do so. Therefore, it is generally advisable to ensure that responsibility for ongoing compliance is allocated to someone, and that there is a mechanism for checking on progress. As part of this process, businesses should seek to build awareness of data protection and privacy expectations and requirements among their staff members, and to ensure that the operational impact is well understood by staff who process personal data.

Last, but by no means least, businesses should see this as an opportunity. Lawmakers are taking privacy and data protection seriously because the public increasingly does so too. A well-planned and well-executed privacy compliance programme can provide a competitive advantage by helping a business to ensure that its customers, suppliers and employees feel confident in allowing that business access to their data – which is increasingly the lifeblood of today's digital world.

**Dr. Detlev Gabel** is a partner in the Frankfurt office of White & Case and is the global head of the Firm's Data, Privacy & Cyber Security Practice. Detlev advises multinational clients on a broad range of data protection and cybersecurity matters, including European and German data protection law compliance, cross-border data transfers and data breach response issues.
Detlev frequently publishes and speaks on topics relating to the aforementioned areas. Notably, he is the co-editor and co-author of highly regarded treaties on data protection law and cybersecurity law, and lectured for almost 10 years on data protection law at the University of Oldenburg, Germany, in a course leading to a Master of IT Law.
*"Detlev Gabel is a top-rated data protection lawyer who advises clients from a range of industries." – Chambers and Partners 2019.*

**White & Case LLP**
Bockenheimer Landstraße 20
60323 Frankfurt am Main
Germany

Tel: +49 6929 9940
Email: dgabel@whitecase.com
URL: www.whitecase.com

**Tim Hickman** is a partner in the London office of White & Case, is dual-qualified in England & Wales and the Republic of Ireland, and advises on all aspects of UK and EU privacy and data protection law. Tim has significant experience of working with a wide range of clients in the EU, Asia and the US.
He has spent time on secondment at Google, advising on cutting-edge privacy and data protection issues. He has also spoken at several events at Harvard Law School, and he delivered the closing address at the Harvard European Law Conference 2019.
*"Tim Hickman's knowledge of data protection law is second to none. He is also personable and easy to work with … Clients appreciate the examples he provides, making the advice more tangible." – The Legal 500 2020.*

**White & Case LLP**
5 Old Broad Street
London EC2N 1DW
United Kingdom

Tel: +44 7532 2517
Email: tim.hickman@whitecase.com
URL: www.whitecase.com

With one of the largest and most experienced data privacy and cybersecurity groups in the world, White & Case's global team is on hand to guide clients through the relevant data protection legislation in the jurisdictions in which they are active. Seamlessly working with their counterparts in other practice areas, our global team has the depth of resources to provide integrated, creative and practical advice on the privacy-related concerns faced by our clients, wherever they are located.
Our experience spans the full range of industry sectors including financial institutions and banking, biotechnology, pharmaceuticals and chemicals, construction and engineering, consumer goods and retail, automotive, hotels and leisure, IT, telecommunications, internet and social media, manufacturing and electronics, publishing and media.

**www.whitecase.com**

WHITE & CASE

# Privacy By Design as a Fundamental Requirement for the Processing of Personal Data

FABIAN PRIVACY LEGAL GmbH

Daniela Fábián Masoch

*Privacy by design ("PbD") is a fundamental requirement for privacy-compliant processing of personal data and is, in principle, a well-known approach. Nevertheless, PbD is often not consistently implemented, in some cases leading to significant consequences and costs for organisations. This article describes the concept of PbD and its practical implementation under the application of the European Union ("EU") General Data Protection Regulation (EU) 2016/679 of 27 April 2016 ("GDPR").*

## 1 Introduction

The ongoing development of new and complex technologies such as artificial intelligence ("AI"), blockchain, or the Internet of Things ("IoT") and their increasing use, as well as ongoing digitisation and centralisation of data management, are leading to increasingly sophisticated ways of automating the processing of enormous amounts of data, facilitating data flows and availability, profiling consumers, customers, patients, or job applicants, and making automated decisions.

To reap the benefits of these technologies, digitisation, and new business models in connection with the processing of personal data, those who develop or deploy them must consider and implement applicable data protection principles and requirements through appropriate and adequate technical and organisational measures from the outset, already at the design stage, and continuously monitor, adjust and update them throughout the lifecycle of the system, product, or process.

With this PbD approach, a company can ensure compliance with legal requirements, meet the expectations of individuals and stakeholders, build trust, make strategic and operational decisions with foresight and efficiently implement business processes. This can include, for example, storing data on servers in the EU or Switzerland instead of in the USA or purchasing software with integrated data protection principles.

PbD has become a critical factor in building and maintaining trust, competitiveness and success in the marketplace.

## 2 The Concept of PbD

The concept of PbD is a fundamental requirement for the effective implementation of data protection. In essence, PbD requires that controllers consider data protection principles and requirements both at the design stage of systems, processes, products or services that involve the processing of personal data, and throughout the lifecycle of personal data, and that they provide for appropriate technical and organisational measures ("TOMs") to implement data protection requirements and protect the rights of data subjects. Controllers must be proactive and anticipate potential privacy intrusions before they occur.

One of the fundamental elements of PbD is "privacy by default". This concept requires that the controller implements appropriate TOMs to ensure that, by default, only personal data that is necessary to fulfil the specific purpose is processed. PbD must be implemented in terms of the amount of data collected, the scope of its processing, the duration of its storage, its security, and its accessibility.

While the concept of PbD has long existed as good practice, it was introduced as a legal obligation for controllers in Art. 25 GDPR, with significant fines for non-compliance. In introducing the PbD concept, the legislator primarily wanted to emphasise that it is not enough to set standards, and that the controller must also *implement* these standards in an effective and verifiable manner. Other laws have also adopted the concept of PbD, most recently the new Swiss Federal Act on Data Protection ("nFADP"), which is expected to come into force in 2022. However, unlike the GDPR, under the nFADP a breach of the new PbD obligation will have no direct consequences.

However, neither the GDPR nor the nFADP specify how the controller should implement PbD in practice.

So far, the introduction of processes and the designation of responsibilities for the systematic and timely assessment of the planned data processing, the technologies and systems used for this purpose and the data protection risks for the data subjects have proven effective. This risk assessment aims to identify the technical and organisational measures required to effectively integrate data protection principles and requirements into the design of the respective products, systems or processes and to protect the privacy of the data subjects. Risks to data subjects include, for example, excessive collection and disclosure of personal data, processing of data for purposes other than the original purpose, unlawful processing, as well as loss, destruction or alteration of data.

Such a risk assessment, coupled with a compliance assessment, is required for any processing of personal data, including, for example, the implementation of a Customer Relation Management ("CRM") or HR data management system or the outsourcing of data processing, regardless of the technology used or the sensitivity of the data. While similar, this risk and compliance assessment is not a data protection impact assessment ("DPIA") as required under Art. 35 GDPR.

A controller must conduct a DPIA only if the processing is likely to present a high risk to data subjects' rights and freedoms. A DPIA is a broader assessment that goes beyond a compliance assessment by evaluating the residual risks to data subjects, taking into account the TOMs embedded in the design of the product, system or process. If the residual risk is still considered high, the controller must take further measures to mitigate the risk. If this is not possible, the controller must consult the data protection authority or refrain from processing. A DPIA will be regularly required for digital health solutions

where health-related data or other special categories of data are processed. A DPIA will also be regularly required for the use of innovative or combined technologies and extensive profiling.

## 3 Implementing PbD In Practice

### 3.1 Technical and organisational measures

The controller must implement TOMs both at the time of determining the means of processing and during the processing itself. The TOMs must be adequate and appropriate to:

- effectively implement data protection principles, such as data minimisation, lawfulness, transparency, confidentiality, purpose limitation, data integrity, storage duration, security, as well as the requirements concerning commissioned data processing and cross-border data transfers;
- integrate the necessary safeguards into the processing to meet the requirements of the GDPR; and
- protect the rights of data subjects.

A measure is adequate if it considers state of the art, the cost of implementation, the nature, scope, context and purposes of the processing, and the risks of varying likelihood and severity to natural persons' rights and freedoms.

**Technical measures** may include, for example:

- robust encryption methods for systems and data;
- pseudonymisation or aggregation of the data;
- access authorisations and restrictions;
- user authentication;
- firewalls; and
- automated deletion concepts.

**Organisational measures** may include, for example:

- the assignment of responsibilities for the effective implementation of data protection requirements;
- the implementation of enforceable policies and procedures for handling and documenting data privacy violations and requests for information from data subjects, risk management, third-party vendor management, data transfer management, and the documentation of processing activities;
- the implementation of training and controls; and
- the establishment of processes to ensure data protection rights, such as revoking consent or requesting erasure of the data.

### 3.2 Data Protection Management System (Fig.1)

One effective way to implement PbD in practice is to build a data management and risk assessment programme with responsibilities and a process to systematically identify, evaluate, address and mitigate potential privacy and security risks associated with the collection and processing of personal data. A Data Protection Management System should include the following elements:

- a documented ***commitment*** by the company's management to establish and enforce high standards of data protection for the company, to integrate data protection into the corporate culture and embed the data protection principles in the design and implementation of corporate policies, data protection management systems, business practices, services and products;
- the appointment of a data protection officer or advisor and the allocation of ***responsibilities*** at all levels of the organisation, including business units and functions, for the effective implementation of data protection requirements;
- the establishment of a data protection ***framework*** with enforceable data protection policies and guidelines that attach appropriate importance to data protection and regulate the collection, processing, transfer, storage and deletion of data, as well as mechanisms to monitor implementation and compliance with standards and rules;
- the application of appropriate ***processes*** to ensure that data protection principles and requirements are adequately taken into account and integrated into data processing procedures and that the PbD principle is thus lived;
- the introduction of ***records of processing activities*** ("RoPA");
- ***risk management*** with risk assessments, compliance checks and, where appropriate, data protection impact assessments;
- ***third-party management*** and ***data transfer governance***;
- regular and documented ***awareness*** campaigns and conducting employee ***training***; and
- regular and documented ***monitoring and controls*** through self-assessments and audits to verify the effective implementation of the data protection management programme and compliance with legal requirements and internal policies and directives.

### 3.3 Data protection considerations and design strategies

**Applicable laws**

The controller must clarify the applicable laws and regulations. In particular, organisations outside the EU must determine whether the GDPR applies to them and their activities. The controller should also check whether industry-specific codes of conduct, certification systems, regulatory decisions or guidelines apply to the planned data processing and take into account ethical considerations.

**Involved parties**

It is then necessary to identify which parties are involved in the data processing or the development and use of the system, service or product, and their role (e.g., controller or processor). Several parties may be jointly responsible for the data processing. Identifying the data controller, i.e., the party that alone or jointly with others decides the means and purposes of data processing, is essential to determine who is responsible and accountable for compliance with data protection requirements under the GDPR.

**Legal justification**

For all personal data processing, controllers must rely on one of the legal bases set out in Arts 6 and 9 of the GDPR, the most used of which are: legitimate interest; performance of a contract; legal obligation; or consent.

In health or medical apps collecting and processing special categories of patient or consumer data, the processing of this data will regularly require the data subjects explicit consent. In this case, consent must be voluntary and specific to each functionality that serves a distinct purpose. Consent must further be based on prior information. In the case of special categories of data, the use of cookies or location data, the data subject must provide explicit consent through positive action, such as downloading the app and ticking a consent box. Also, controllers must have a procedure in place that allows for easy withdrawal of consent and, on the other hand, ensures that in the event of withdrawal, the data collected will not be further processed.

**Proportionality and data minimisation**
Personal data must be adequate, relevant, and limited to what is necessary for the purposes for which it is processed. This means that systems, apps and devices that store or process personal data should be set up so that only the data necessary for the individual purpose or the proper functioning of the system, app or device is stored and processed.

The principle of data minimisation can be achieved in different ways, for example, by reducing the amount of personal data collected and processed or by making it more difficult or impossible to assign the data to an individual.

Depending on the functionalities of the system, app or product and the purpose of the processing, the controller must therefore assess for each data set to be collected whether this data is indeed necessary to fulfil the purpose or whether the purpose can be fulfilled with less data (reduction of data volume) or pseudonymised/anonymised data (making identification difficult or impossible). A further distinction must be made between mandatory data and voluntary data that can be additionally provided for the use of certain functionalities.

Another measure that the controller can take to achieve the data minimisation requirement is to prevent the linking of personal data stored in different systems for different purposes.

**Transparency and fair processing**
Personal data must be processed transparently and fairly. Data subjects should have full transparency and control over the processing of their data and understand what data is being processed, why, by whom, where and for how long, and how they can exercise their data protection rights. The processing of personal data should neither violate applicable laws, nor be unexpected to the data subject.

The privacy notice should be easily accessible to data subjects at any time, before the collection of personal data and throughout the processing. Users of apps, for example, should be notified before the download of the app. The notice should be easy to understand and, where appropriate, translated in different languages.

**Confidentiality and access to personal data**
Personal data must be kept strictly confidential and may only be provided or disclosed to individuals on a need-to-know basis to fulfil the legitimate purposes for which the data was collected.

Special attention is required for centralised data management systems. In this case, the controller should establish data access and restriction policies and limit the access through technical means.

**Purpose limitation**
Personal data shall only be collected for specified, explicit and legitimate purposes and shall not be further processed in a way incompatible with those purposes.

The controller should determine the processing purposes and communicate them to the data subjects. The functionalities of the system, app or product should be set up to ensure that personal data is only processed for these purposes. The controller must also determine who should have access to which data for which purposes and implement these regulations through technical measures as well as instructions, training and controls.

If the personal data is to be processed later for purposes other than those communicated, it should be anonymised, unless there is another legal basis for this secondary use. In any case, data subjects should be informed in advance about the use of their data for any secondary purpose and, unless there is another legal basis, their consent should be obtained.

**Data quality**
The personal data stored must be accurate and, where necessary, kept up to date, and all reasonable steps must be taken to ensure that inaccurate personal data is erased or rectified without delay.

The controller must have mechanisms in place to ensure that data is accurate at the time of collection and is not unlawfully altered thereafter. There must be a mechanism to correct or delete inaccurate data.

**Data retention**
Personal data must be kept in a form that permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed, unless regulatory or legal requirements necessitate a longer or shorter retention period.

The controller should establish a data retention and deletion policy and determine a retention period for each data set based on the purpose of the processing and, where applicable, legal and regulatory retention periods.

The controller must also define mechanisms, including automated solutions where appropriate, and responsibilities for the effective deletion of data. If the data cannot be deleted, it must be anonymised or, if this is not possible, pseudonymised.

**Data security**
Personal data must be processed in a manner that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage, using appropriate TOMs. These measures should include data integrity and confidentiality, availability, resilience and traceability, and ensure a level of security appropriate to the risk to the rights of data subjects.

Appropriate control access mechanisms and authentication measures should be embedded in the system infrastructure to detect and monitor unauthorised access to data. Personal data should be protected by strong and robust state-of-the-art encryption, both in transit and in storage. Special attention is required when data is stored in the cloud.

**Privacy rights**
Data subjects have various data protection rights, including the right to information, access, rectification and erasure, restriction of processing, data portability and the right to object to automated individual decision-making. They also have the right to complain to the competent supervisory authority if they feel their rights are being violated or their data is not adequately protected. The controller must define processes to ensure that data can be corrected, deleted or transferred at the data subjects' legitimate request. For apps in particular, the controller should consider whether users should be able to exercise their rights directly through the app, if necessary, by accessing the data and correcting or deleting it if inaccurate.

**Data processing by third parties and cross-border data transfers**
Depending on the roles of the contributors in the development, management and use of the system, app or product and the data processed, the controller must establish appropriate contractual obligations to ensure data protection.

Before sharing any personal data with a processor, the controller must verify that the processor implements appropriate TOMs to ensure compliance with the data protection requirements and data subjects' privacy rights.

If personal data is to be transferred to third parties outside the European Economic Area ("EEA") to a country without a formal adequacy decision by the European Commission,

appropriate safeguards, such as EU standard contractual clauses ("SCCs"), must be implemented to legitimise cross-border data transfers, unless an exemption pursuant to Art. 49 GDPR applies, such as the explicit consent of the data subject.

Before transferring the data, the controller, respectively the data exporter, must check whether the destination country ensures an adequate protection level equivalent to that in the EU. If this is not the case, the data exporter should consider storing and processing the data in the EU or an adequate country. If this is not an option, additional contractual, technical and organisational measures must be taken, such as pseudonymisation or encryption of the data while keeping the encryption key in the EU and separate from the service provider.

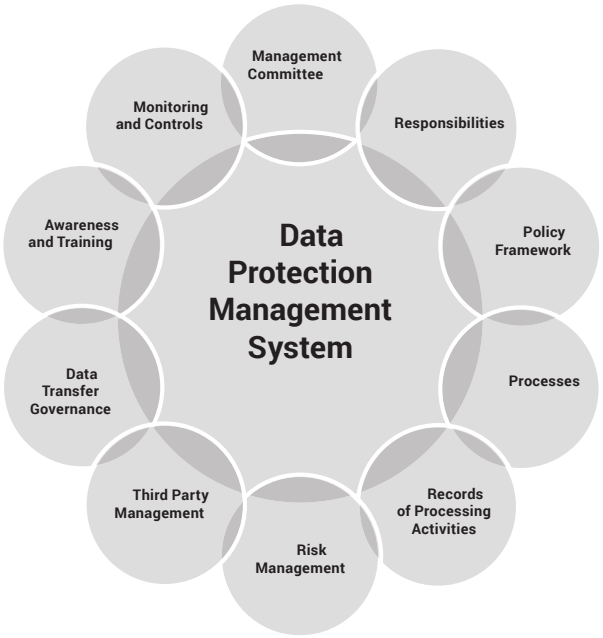
## 4 Conclusion

Consistent and sustainable compliance with data protection requires the strategic and conceptual integration of data protection principles in all business practices, the organisational structure, the development of rules, IT systems and products.

To fully exploit the benefits of new technologies and ensure their effectiveness, it is essential to embed fundamental data protection principles into the design of these solutions, taking into account organisational, process and system-related risks, as well as risks to the rights of data subjects.

PbD is not only required by the GDPR and partly by laws of other countries outside the EEA. It is a prerequisite for the effective and sustainable implementation of data protection, the basis for the smooth functioning of data protection management, and a critical factor in achieving the necessary trust of employees, customers, patients and consumers, public authorities, business partners and other stakeholders in the use of new technologies and the processing of their personal data.

**Fig.1**



**Daniela Fábián Masoch** is the founder and executive director of FABIAN PRIVACY LEGAL GmbH, a boutique law firm specialised in international, European and Swiss data protection law, governance, risk management and programme implementation. Daniela is a Swiss attorney-at-law, certified Privacy Professional and ISMS 27001 Lead Auditor, with 30 years of professional experience. She advises multinational companies in the EU, Switzerland and the USA on data protection and security issues in various industries, mainly in the pharmaceutical and medical device industries.

Daniela supports her clients in evaluating, developing, implementing and monitoring data protection strategies, governance models and global data protection programmes and data transfer mechanisms with a pragmatic approach.

Before starting her own company in 2015, Daniela held various positions at Novartis, most recently as Global Head of Data Privacy, where she was responsible for the Group's strategic direction on data privacy, as well as establishing, implementing and overseeing the global data privacy function, global data privacy management programme and binding corporate rules.

Daniela is a member of various data protection associations and a lecturer at FernUni Switzerland for the CAS Data Protection and at Swiss Health Quality Association ("shqa") for Digital Marketing.

**FABIAN PRIVACY LEGAL GmbH**
Bäumleingasse 10
4051 Basel
Switzerland

Tel: +41 61 544 44 01
Email: daniela.fabian@privacylegal.ch
URL: www.privacylegal.ch

FABIAN PRIVACY LEGAL GmbH is a boutique law firm specialising in international, European and Swiss data protection law, governance, risk management and programme implementation.

Our strengths are the combination of expert knowledge and practical in-house experience, an excellent network with industry groups and data protection associations, and close cooperation with data protection, cybersecurity and cybercrime experts worldwide as well as corresponding law firms advising on local legal issues. We approach mandates with a global, solution-oriented and practical approach to deliver pragmatic and sustainable solutions.

Our clients are large and small companies in a wide range of industries, including pharmaceuticals, biotechnology and medical devices, technology, consumer goods, luxury goods, food and beverages, transport and logistics, automotive, insurance, financial institutions and the chemical industry.

**www.privacylegal.ch**

# Initiatives to Boost Data Business in Japan

Anderson Mōri & Tomotsune

Takashi Nakazaki

## I Introduction

In an effort to increase data business in Japan, the government has enacted new legislation and established various supporting guidelines in recent years. In particular, the government issued, and continues to update, guidelines focusing on private businesses utilising big data and artificial intelligence ("**AI**") to clarify and analyse legal issues. In addition, the government has issued specialised guidelines for various industries, such as agriculture and gas. Furthermore, the government is considering ways to strengthen regulations regarding competition policy.

## II New Protected Data Category – "Limited Provided Data"

### 1 Legal protection for data under Japanese law

Data is intangible, and because it is not the subject of rights under the Civil Code, such as ownership or possession, usufruct, or security interest, it is not possible to prescribe the existence or absence of rights pertaining to data based on concepts of ownership or possession (see Articles 206 and 85 of the Civil Code). As described below in Part IV (2) – *Concerns over damage caused by leaks and unauthorised use of data*, the cases in which data is subject to legal protection (either as intellectual property, or as a trade secret under the Unfair Trade Practices Act) are limited, so the protection of data is generally achieved through contracts between the interested parties.

Although data can be protected by copyright, patent, and trade secret law, these rights may not adequately protect data for the following reasons.

Works that are subject to protection by copyright are prescribed as productions that express thoughts or sentiments in a creative way (Article 2(1)(i) of the Copyright Act). In many cases, it would be difficult to find a creative element in a collection of data, such as data that is mechanically generated by devices including sensors, cameras, or the usage logs of smartphones, etc.

Also, inventions that are subject to patent protection are highly advanced creations of technical ideas utilising the laws of nature. Cases in which data would be subject to patent protection are limited.

By contrast, data may be subject to legal protection as a trade secret under the Unfair Trade Practices Act if the data embodies know-how of an entity involved in the creation of data or in the distribution or utilisation of data (such as know-how related to production methods in the manufacturing industry, data cleansing by sensor manufacturers, or utilisation of data by service development providers), and the data: (i) is managed as a secret; (ii) has utility; and (iii) is not in the public domain. Yet data will not necessarily be protected as a trade secret if it will be distributed during a transaction.

The following table provides an outline of intellectual property rights, etc. relating to the protection of data:

| Type of right | Nature of right | Ability to be used for data protection |
|---|---|---|
| Copyright | The work must be a production in which thoughts or sentiments are creatively expressed and which falls within the literary, academic, artistic or musical domain (Article 2(1)(i) of the Copyright Act). | The cases in which mechanically generated data can be found to have a creative element are limited. |
| Patent | A patent right for a highly advanced creation of technical ideas using the laws of nature that is industrially applicable will become effective upon registration of the invention's establishment. Patent examination is not available for inventions that do not have novelty or an inventive step (Article 2(1), Article 29(1), and Article 66(1) of the Patent Act). | Regardless of the method of processing or analysing data, the cases in which the data itself can be found to be a highly advanced creation of technical ideas utilising the laws of nature are limited. |
| Trade secret | Information is a trade secret if it: (i) is managed as a secret; (ii) has utility; and (iii) is not in the public domain. In the case of a statutorily proscribed act, such as acquiring a trade secret by unfair means (unfair competition), the aggrieved party may seek an injunction, damages, or criminal penalty (Article 2(6), Article 2(1)(iv) through (x), Article 3, Article 4, Article 21, and Article 22). | Data can enjoy legal protection if the elements in (i) through (iii) are satisfied. |

## 2 Protection under the Unfair Competition Prevention Act

As stated above, data that satisfies the three elements contained in Article 2 of the Unfair Competition Prevention Act will enjoy protection as a "trade secret".

However, because there has been continued innovation in information technology, such as Internet of Things ("**IoT**") and AI, and the source of companies' competitive advantage is starting to become data and its utilisation, it is necessary to establish a business environment that enables the safe and reliable utilisation of data. In response to these changes, the government recently enacted the Act to Partially Amend the Unfair Prevention Act, Etc. in May 2018 (the "**Amended Unfair Competition Act**"). The Amended Unfair Competition Act introduced remedial measures in civil law, such as injunctions against the unauthorised acquisition or use, etc. of data that is provided in a protected form such as by ID or password, on the basis that this activity constitutes "unfair competition".

The data that is subject to protection under the Amended Unfair Competition Act is "limited provided data", which means "technical or business information accumulated or managed in significant volume by electromagnetic means as information provided to certain persons as a business (other than information managed as a secret)" (Article 2(7) of the Amended Unfair Competition Act).

The elements of applicable data and the unfair competition activities that are subject to the new regulations are as follows:

### Elements of data that are the subject of protection

Data that meets the following elements should be subject to protection:

**(i) Managed with technology**

The data must be managed by appropriate electromagnetic access control means (such as ID and password, dedicated network, data encryption, or scrambling) for provision to only a certain limited scope of persons. Further, there must be a clearly recognised management intention that third parties, other than those persons contemplated in the contract with the data provider, may not use or be provided with the data.

**(ii) Limited provision to outside parties**

Unlike "trade secrets", which are managed as a secret and are used in-house by the owner or, as an exception, disclosed to limited persons who have executed a confidentiality agreement, the data must be of a kind that is intended to be optionally provided to certain outside parties in response to their requests.

**(iii) Utility**

The data must be recognised as having commercial value, by stripping the data objects of any illegal or immoral content, and by combining the data objects together.

### Unfair competition activities regarding data

The following activities would be deemed as "unfair competition activities" and remedial measures would be introduced for these activities:

**(i) "Unauthorised acquisition" type**

Where an unauthorised outside party acquires data through a management breach or, having so acquired the data, uses the data or provides it to a third party (Article 2(1)(xi) of the Unfair Competition Prevention Act). In this context, "management breach" means an act that is harmful to the data provider's management of the data (such as unauthorised access or trespassing), or an act equivalent to fraud, etc. in causing the data provider to provide the data after removing technical management measures (such as acts of fraud, violence, or threat).

**(ii) "Extreme bad faith" type**

Where data that is subject to a condition that provision to third parties is prohibited, is acquired from a data provider and is used in activity that is equivalent to embezzlement or defalcation (a form of activity that betrays an advanced relationship of trust between parties to a service agreement, etc.) with the purpose of obtaining unjust profit or causing damage to the data provider (a "profit or harm motive"), or where the data is provided to a third party for a profit or harm motive (Article 2(1)(xiv) of the Amended Unfair Competition Act).

**(iii) "Subsequent acquisition" type**

Where a person acquiring data knows that an improper act took place in relation to that data and nevertheless proceeds to acquire that data, or uses the data so acquired or provides it to a third party (Article 2(1)(xii) and (xv) of the Amended Unfair Competition Act).

Where a person acquiring data did not know at the time of the acquisition that an improper act took place in relation to such data, and, after subsequently becoming aware of such improper act (i.e., acting in bad faith), provides the data to a third party (Article 2(1)(xiii) and (xvi)). Cases where the data is provided within an authorised scope prescribed in a transaction that predates the subsequent acquirer's bad-faith action are excluded.

## III Protection under the Act on the Protection of Personal Information

The Japanese government intends to strengthen legal protection for personal data by amending the Act on the Protection of Personal Information (the "**APPI**"). The APPI was amended in 2020. The amendment, except for certain provisions, will take effect on April 1, 2022. This amendment is a follow-up on the Japanese government's policy to review the legal system every three years, as stipulated by the 2015 amendment to the Act, which came into full force on May 30, 2017. The 2020 amendment makes reforms to the Act to strengthen the protection of the rights of principals who may be identified by personal information, as well as the supervisory and enforcement powers of the Personal Information Protection Commission of Japan (the "**PPC**"). The amendment also aims to promote the utilisation of data in society. The contents of the amendment are the following items:

### 1 Strengthening data protection

(i) The amendment introduces a new concept of personal information (*kojin-kanren-joho*). Under the APPI, personal information is defined as information about a living individual that can identify the specific individual by name, date of birth, or other description contained in that information. Under the amendment, certain non-personal information, such as cookies and IP addresses, would also be subject to third-party provision regulations, if the receiving third party is likely to receive the data as personal data. In that case, the providing party must confirm that the recipient has obtained the consent of data subjects to the provision of their data as personal data. This regulation would affect the online advertising industry.

(ii) Under the current APPI, any personal data that is prearranged to be erased within six months from acquisition is not "retained personal data" and is therefore not subject to data subjects' rights on retained personal data. The amendment will remove the six-month qualification, so that any personal data is "retained personal data" regardless of the data retention period.

(iii) Under the current APPI, data subjects have the right to demand the termination of use of, deletion of, and cessation of third-party transfer of their retained personal data, only if that data was used for purposes other than those about which the data subjects were notified, was collected by deceit or other improper means, or was provided to a third party in violation of the APPI. The amendment would allow data subjects to demand cessation of the utilisation of their personal data when their personal rights and interests are at risk of harm, such as when data is stored even after the business operator ceased using it for its stated purposes.

(iv) In contrast to the current APPI, the amendment would clarify that a business operator must not utilise personal data in ways that encourage or cause unlawful or undue use. Details of these obligations are not available currently; however, the amendment might possibly restrict data business in Japan, depending on what types of utilisation would be considered undue by the PPC, the regulator of data protection in Japan, or other regulators.

(v) The provision of personal data to third parties under the current APPI generally requires the consent of data subjects, although certain exceptions apply. One exception that is available to a limited number of entities is the opt-out scheme, which requires filing with the PPC and making certain information available to data subjects. The amendment would strengthen regulations applicable to such entities and, moreover, restrict the range of personal data that may be provided to a third party based on the opt-out scheme. The following specific types of personal data may not be provided to third parties based on the opt-out scheme: (1) personal data collected by deceit or other improper means; and (2) personal data received from another person based on an opt-out scheme of that other person.

### 2 Promoting data business

The current APPI provides an anonymisation system for personal data to promote data business, but many companies have not utilised the system due to certain obligations and unclear standards on anonymising. However, many companies process personal data by replacing names with ID for data security. The amendment describes that such processed personal data would be considered pseudonymised information. A business operator handling personal data that is considered to be pseudonymised information would not need to comply with certain obligations under the APPI. The use of pseudonymised information is limited to the internal use of the business operator, and the provision of pseudonymised information to third parties is prohibited.

### 3 Data breach notification requirements

Under the current APPI, by contrast to the GDPR, a business operator is not legally required to submit a report of a data breach to the PPC or to notify affected data subjects, but is strongly encouraged to do so. The amendment would introduce mandatory obligations to report data breach incidents to the PPC and notify the affected data subjects if the data subjects' rights and interests are likely to be infringed.

### 4 The PPC's stronger authority relating to foreign entities and international data transfer

(i) Under the current APPI, the PPC has no authority to compel an entity located in a foreign country to submit reports, or to issue orders to that entity. The amendment would provide that authority.

(ii) The amendment would strengthen a business operator's obligations in transferring personal data to a third party located in a foreign country. Under the APPI, in addition to the general requirements for third-party transfer, prior consent of data subjects specifying the receiving country is required for transfers to a third party in a foreign country unless the foreign country is white-listed under the enforcement rules of the APPI, or unless the third party receiving personal data has established similarly adequate standards for privacy protection as specified in the enforcement rules of the APPI. Currently, only EU countries are specified as white-listed countries based on the adequacy decision of January 23, 2019. Some Japanese companies transfer personal data to foreign entities in non-EU countries by taking necessary steps to ensure that those entities establish a system that conforms to standards prescribed by the PPC. Under the current APPI, the transfer actions would not be disclosed and a data subject would have no power to know the situation and would have difficulty exercising his/her rights. The amendment would enable the relevant data subject to request the providing party to disclose information regarding the actions so taken.
The guidelines for the amendment will be available in the summer of 2021.

## IV Guidelines Focusing on Big Data

The government's guidelines focus on matters that should be included in data contracts, meaning contracts relating to the utilisation, processing, transfer, and other handling of data. The guidelines have a view towards promoting reasonable negotiations and execution of contracts, reducing transaction costs and diffusing data contracts, etc. in light of the fact that data contracts tend to be incomplete contracts that fail to cover any events that may occur after the execution thereof. The basic ideas are as follows:

### 1 Purpose

Because data contracts have not been broadly executed in general and contractual practices have not become standardised, data contracts are likely to cause various problems when they are executed in the future. The guidelines are aimed, with respect to data contracts that have the characteristics described above and for which no standard form is established, at reducing transaction costs and diffusing data contracts in order to promote the effective use of data. The guidelines accomplish these goals by presenting major issues and questions for each type of contract, and by providing examples of contractual terms that are easily accessible to the public and factors to be considered when preparing those terms.

The Ministry of Economy, Trade and Industry and other authorities have already published two sets of guidelines related to data contracts. First, the "Contract Guidelines for Promotion of Data Transaction", published in October 2015, presented the conditions, points and other matters relating to the provision of data by rights holders of the data, on the assumption that the rights holders can be clearly identified from among the interested parties. Second, the "Contract Guidelines on Data Utilization Rights ver. 1.0", published in May 2017, presented the consultation process for determining the holders of utilisation rights and the process for determining the contractual utilisation rights.

However, the two sets of guidelines above were not intended to comprehensively present the types and terms of all data contracts. Further, it is apparent from the rapid progress of AI and IoT technologies in recent years that the environment surrounding data contracts has evolved dramatically on a daily basis, against a background of technological innovation that enables the collection, processing and analysis of enormous amounts of data. Therefore, the practice of drafting data contracts, and the guidelines for the discipline of that practice, must also respond to those drastic changes. Typical examples of the difficulties in this area are: (1) issues related to so-called data ownership; (2) issues of how to handle derived data when a contracting party creates, processes, or integrates new data; and (3) issues of how to cope with the increase in new types of contract in which data is shared and used by platforms that go beyond the existing boundaries of companies and affiliates. In addition, users of the previous guidelines have not only raised questions about the present situation where data distribution is taken as a given, but also made requests for more clear explanation on how the guidelines should apply to specific cases (use cases, etc.) and on points of concern in the handling of personal information and cross-border transactions.

Accordingly, these guidelines, which cover contracts regarding data, the value of which is often uncertain at the stage of execution, examine the positions of each party to those contracts based on the discussions of professionals on concrete cases, list matters that should be generally included in contracts after organising them by contract types, and provide examples of contractual terms and factors to be considered when preparing those terms.

Also, the Ministry of Economy, Trade and Industry is focusing on the relationship between AI and ethics and intends to issue the guidelines on AI governance related to ethical issues and legal issues within 2021.

## 2 Importance and issues of data distribution and utilisation

Recently, the amount of data related to transactions has explosively increased in connection with the promotion of, among other things, IT adoption in those transactions. In some cases, data creates added value when combined with other data, and the combination of multiple data across industries especially is expected to lead to open innovation. To enhance the added value of data and to strengthen competitiveness, it is important to expand the subjects and types of data to be used and to utilise that data in various combinations.

### (1) Promotion of data utilisation

In many cases, data itself is not valuable, and value is created only after processing and analysing data and developing methods for utilising the data for business activities. Therefore, it would be desirable, when conducting contractual negotiations, to empower the parties that have the method or ability to utilise the data, encourage those parties to utilise the data, and distribute profits gained from the data utilisation among the parties.

Certain types of data create sufficient value only when collected in a certain amount. For example, real-time driving data of vehicles can be used for congestion analysis when the data of a large number of vehicles is collected, and that data creates value that cannot be realised simply by analysing the data of each vehicle. Similarly, in the case of data regarding the operational status of machine tools, etc., it becomes possible to perform statistically meaningful analysis on the operation of those tools only by accumulating data from a large number of tools. In these types of cases, the party that can collect and utilise the largest volume of data should be authorised to use the data.

In connection with allocation of the utilisation rights, it is also important that the resulting interests are distributed among the parties in an appropriate manner. In order to collect, process, and analyse data and develop utilisation methods, etc., parties must make hardware investments, such as sensors and servers, as well as human investments, such as data analysts. It is desirable to provide incentives for these investments and to grant the parties making those investments appropriate profits (returns).

### (2) Concerns over damage caused by leaks and unauthorised use of data

There are certain risks in the distribution and utilisation of data. In general terms, data can be easily duplicated and, if there is no appropriate management system, may be leaked to the outside through unauthorised access. Therefore, when data contains a company's confidential information, the company may be anxious that trade secrets and know-how might be leaked out of the company through the provision of the data. Moreover, if any personal information is included in the data, not only may the industrial competitiveness of the parties be diminished, but privacy rights may also be infringed.

In considering data distribution and utilisation in individual cases, it is essential to pay careful attention to the concerns about these risks. The risks may be minimised through appropriate contractual and technical measures, so the parties should understand those various measures to correctly evaluate the risks and benefits and to execute reasonable data contracts. The methods for preventing any leaks or unauthorised utilisation of trade secrets and know-how, etc. are described in section II above.

### (3) Increased complexity and sophistication of contracts and significance of these guidelines

If the parties to data contracts, which are a new type of contract for which the matters to be decided are becoming increasingly complex and sophisticated, can build reasonable business relationships for data distribution and utilisation at a low cost, the competitiveness of the parties as well as national competitiveness would increase, in combination with the application of laws, including the Act on Prohibition of Private Monopolization and Maintenance of Fair Trade (the "Antimonopoly Act") and the Unfair Competition Prevention Act.

However, in light of the principle of freedom of contract, matters such as the selection of counterparty, determination of contents, and method of contracting are left to the choice of the contracting parties. Therefore, these guidelines only indicate the matters to be set forth in contracts and do not, as a matter of course, restrict any freedom of contract.

Specifically, for the purpose of generally diffusing data contracts among various transactions, these guidelines introduce matters to be included in contracts executed between business operators for the distribution, utilisation, sharing, etc. of data.

In order to increase the sophistication of contracts, it is necessary to remember that utilisation rights can be freely stipulated by contract. Since data is intangible by nature and is not subject to ownership, the utilisation rights can be freely determined between the parties by contract. Therefore, to increase the sophistication of data contracts, the parties should flexibly determine the conditions of use and should set forth specific details of the utilisation rights and other matters, with reference to these guidelines and taking into consideration the degree of contribution to the creation and utilisation of data and other factors.

**(4) Promotion of innovation**

These guidelines aim to support parties who wish to distribute and utilise data, and to enable the utilisation of new, undiscovered value by not only promoting traditional innovations in which data is utilised through the efforts of individual companies without opening the data, but also by further expanding the possibilities of open innovation.

Another purpose of these guidelines is to encourage the utilisation of data and promote open innovation by providing the concept of data contracts and contract terms, etc. and by giving consideration to various positions.

## V Competition Policy Focusing on Big Data and Platform Business

Potential problems under the Antimonopoly Act can emerge in cases where unilateral contract provisions, etc. are imposed against a backdrop of what amounts to a position of dominance in the negotiation of contracts between large corporations on the one hand, and medium-sized, small, and venture corporations on the other hand, or in cases where the parties conduct exclusive dealing and restrictive trading, etc.

### 1 Abuse of a dominant bargaining position

Abuse of a dominant bargaining position under the Antimonopoly Act (Article 2(9)(v)) can become a problem if there is a relationship of relative dominance between contracting parties. In this regard, the "Guidelines Concerning Abuse of a Dominant Bargaining Position in Service Transactions under the Antimonopoly Act", published by the Japan Fair Trade Commission ("**JFTC**"), state the following views:

(i) In a service transaction, a service provider can suffer undue disadvantage if a service delegator with a dominant bargaining position abuses its superior bargaining position by unilaterally causing a service provider to assign (including through licensing) the service provider's rights in deliverables to the service delegator, or by restricting the use of deliverables, technologies, etc. for other purposes (i.e., secondary use) to an extent not contrary to the purpose of the service transaction, on the basis that the deliverables, etc. have been obtained in the course of the service transaction with the service delegator or have been created at the expense of the service delegator.

(ii) Even under those circumstances, however, abuse of a dominant bargaining position does not arise if consideration for assignment of the rights pertaining to, or for restriction on secondary use of, Derivative Products is paid separately, or if negotiations for consideration are conducted in a manner that includes consideration for the assignment or restriction.

(iii) By contrast, abuse of a dominant bargaining position does arise in service transactions that are unreasonably disadvantageous to the service provider, such as cases where consideration for the assignment, etc. of the rights pertaining to Derivative Products is unreasonably low or where the assignment, etc. of the rights pertaining to Derivative Products is essentially forced.

Accordingly, in contracts regarding the development of AI-based software between Vendors and Users where the terms and conditions are basically entrusted to the independent judgment of each party, abuse of a dominant bargaining position can occur if either party exploits a dominant bargaining position over the other party unjustly in light of ordinary business practices in order to delay the payment of the price, to reduce the price, to conduct a transaction or do-over for significantly lower consideration, or to unilaterally handle rights, etc. pertaining to raw data, a training dataset, a training programme, or a trained model for the use of AI technology (e.g., assignment of such rights and restriction on secondary use). However, abuse of a dominant bargaining position does not emerge in cases where appropriate consideration is paid separately for the assignment of rights or restriction on secondary use, or where negotiations for consideration are conducted in an appropriate manner that includes the consideration for the assignment or restriction, including conditions for income-sharing in secondary use.

### 2 Exclusive dealing and restrictive trading, etc.

Unfair trade practices under Article 19 of the Antimonopoly Act, such as exclusive dealing and restrictive trading, can occur when parties establish terms of use for AI-based software and stipulate contractual provisions for restriction on the use of such software.

In a licensing contract, the following act is, in principle, deemed to constitute an unfair trade practice: imposing an obligation to vest in the licensor or a business operator designated by the licensor the rights in improved technology developed by the licensee, or the obligation to grant an exclusive licence to the licensor with respect to that improved technology. Even if the rights or licensing were shared, that act would be considered an unfair trade practice if the act constituted an impediment to fair competition ((12) of the Designation of Unfair Trade Practices (Fair Trade Commission Public Notice No. 15 of 1982)).

By contrast, imposing an obligation to license the licensee's improved technology in a non-exclusive manner to the licensor does not, in principle, constitute an unfair trade practice if the licensee has the discretion to use the improved technology developed by the licensee. In addition, if the improved technology developed by the licensee cannot be used without the technology licensed by the licensor, it is generally understood that the act of imposing an obligation to assign the rights pertaining to the improved technology to the licensor for reasonable consideration does not constitute an impediment to fair competition. Furthermore, the act of imposing an obligation to report to the licensor any knowledge or experience obtained in the course of using the licensed technology does not, in principle, constitute an unfair trade practice unless, in effect, that obligation requires the licensee to license the know-how acquired by it to the licensor.

### 3 Platform business regulation

The Japanese government intends to introduce new regulations regarding the platform business industry, which includes global IT giants. In December 2019, the JFTC introduced its Guidelines concerning Abuse of a Superior Bargaining Position in Transactions between Digital Platform Operators and Consumers that provide personal information, etc. (the "**Guidelines**"). The Guidelines clarify the JFTC's view that a digital platform operator has a superior bargaining position over consumers who provide personal information because the consumers, who may be subject to detrimental treatment by the digital platform operator, are compelled to accept that treatment in order to use the services provided by the digital platform operator. The Guidelines also explain various examples of abuse of a superior bargaining position in this context, including a digital platform operator that: (i) causes consumers to provide personal information without stating the purposes of the use of that information, such as on a webpage or by other means; (ii) obtains or utilises personal information contrary to consumers' intentions and beyond the scope necessary to achieve the purpose of use, such as by providing consumers' personal information to third parties without consent; (iii) obtains and utilises consumers' personal information without taking precautions necessary and appropriate for ensuring the safe management of that personal information; and (iv) causes consumers who continuously utilise its services to provide economic interests, such as unnecessary personal information, in addition to compensation in exchange for the utilisation of services.

Furthermore, the Japanese government submitted a bill to the Diet aimed at improving transparency and fairness of transactions by digital platform operators. The bill is expected to apply to IT giants such as Apple, Amazon, Rakuten, and Yahoo!, and requires digital platform operators to disclose trading conditions and make prior notifications of amendments to those trading conditions. The bill passed the Diet in May 2020, and will come into effect in 2021.

Outsourcing the creation of programmes is considered to be an "information-based product creation contract" under the Act against Delay in Payment of Subcontract Proceeds, Etc. to Subcontractors (the "**Subcontractors Act**"). Under the Subcontractors Act, a business operator that places an order (the main subcontracting entrepreneur) is prohibited from delaying payment, reducing subcontract proceeds, and engaging in transactions, etc. for significantly low subcontract proceeds.

## VI Information Bank

The so-called "information bank" platform started in 2019. In this new business model, an information bank collects and stores data relating to personal consumers and, based on their consent to the data being shared, the information bank would provide the personal information to businesses in exchange for a fee. The platform could be run by a system development company or a telecommunications provider, for example.

The information bank could hold several types of data, including social network profiles, fitness data tracked through wearable devices, online shopping histories and GPS locations. Individuals would be able to choose the information that they are willing to share, and with whom.

Businesses would be able to gain access to information from other companies and industries, in addition to customer data that they collected on their own. This access will allow businesses to create products and services that are better suited to customers' interests.

**Takashi Nakazaki** is special counsel at Anderson Mōri & Tomotsune, with broad experience in the areas of data protection and privacy (including big data and IoT), information security, intellectual property, licensing, and payment services including cryptocurrency. Further, he has experience working on matters relating to cyber law issues such as cloud computing, domain names, e-commerce, social media and other technology-related areas, telecommunications, labour and general corporate law.

In the area of data protection law, he frequently advises various international and domestic online service companies including operators of online games, online gambling and social networking sites. In addition, he regularly assists the Japanese government in data protection and cyber law areas, including the "National *Omote-nashi* project", "AI & Data Contracts Guidelines" and "AI Governance Guidelines" and leads the Tokyo branch of the International Association of Privacy Professionals (IAPP) as a co-chair. Mr. Nakazaki has been ranked as one of the top lawyers in the data protection and information security field for the last several years.

**Anderson Mōri & Tomotsune**
Otemachi Park Building
1-1-1 Otemachi, Chiyoda-ku
Tokyo 100-8136
Japan

Tel: +81 3 6775 1086
Email: takashi.nakazaki@amt-law.com
URL: www.amt-law.com

Anderson Mōri & Tomotsune is a full-service law firm formed by the merger and consolidation of the practices of three leading Japanese law firms: Anderson Mōri, which established its reputation as one of the largest and most established international law firms in Japan since its inception in the early 1950s; Tomotsune & Kimura, particularly known for its expertise in international finance transactions; and Bingham Sakai Mimura Aizawa, a premier international insolvency/restructuring and crisis-management firm. With a long tradition of serving the international business and legal communities, our superior expertise, coupled with our standing as one of the largest law firms in Japan, translates to not only high-quality services but also time and cost efficiencies, which we share with our clients.

**www.amt-law.com**

ANDERSON MŌRI & TOMOTSUNE

# Australia

MinterEllison

Anthony Borgese

## 1 Relevant Legislation and Competent Authorities

### 1.1 What is the principal data protection legislation?

The *Privacy Act 1988* (Cth) (**Privacy Act**), which includes the Australian Privacy Principles (**APPs**), is the principal data protection legislation.

### 1.2 Is there any other general legislation that impacts data protection?

Yes, other general legislation that impacts data protection include the following:

- *Do Not Call Register Act 2006* (Cth) (**DNCR Act**) stipulates limitations with respect to unsolicited telephone calls;
- *Spam Act 2003* (Cth) (**Spam Act**) sets out rules with respect to commercial messages; and
- *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) contains provisions relating to compliance with the APPs in respect of information obtained under this Act.

There is also the following legislation at the state and territory level:

- *Privacy and Personal Information Protection Act 1998* (NSW);
- *Information Privacy Act 2014* (ACT);
- *Workplace Privacy Act 2011* (ACT);
- *Information Privacy Act 2009* (Qld);
- *Invasion of Privacy Act 1971* (Qld);
- *Privacy and Data Protection Act 2014* (Vic); and
- *Personal Information Protection Act* (Tas).

### 1.3 Is there any sector-specific legislation that impacts data protection?

Yes, there is sector-specific legislation impacting data protection, including those set out below.

For the telecommunications sector:

- *Telecommunications Act 1997* (Cth); and
- *Telecommunications (Interception and Access) Act 1979* (Cth).

For the health sector:

- *My Health Records Act 2012* (Cth);
- *Healthcare Identifiers Act 2010* (Cth);
- *Health Records and Information Privacy Act 2002* (NSW); and
- *Health Records Act 2001* (Vic).

For the banking, insurance and superannuation industries:

- *Prudential Standard CPS 231 (Outsourcing) and Prudential Standard SPS 231* (**Outsourcing**) (together, **CPS 231**); and
- *Prudential Standard CPS 234 (Information Security)* (**CPS 234**),

which are issued by the Australian Prudential Regulation Authority (**APRA**) under:

- *Banking Act 1959* (Cth);
- *Insurance Act 1973* (Cth);
- *Life Insurance Act 1995* (Cth);
- *Private Health Insurance (Prudential Supervision) Act 2015* (Cth); and
- *Superannuation Industry (Supervision) Act 1993* (Cth).

In addition, the *Competition and Consumer Act 2010* (Cth) also applies to specific sectors covered by its consumer data right (**CDR**) regime (commonly referred to as "Open Banking", and further discussed under question 18.2 below).

### 1.4 What authority(ies) are responsible for data protection?

The main authorities include the following:

- The Office of the Australian Information Commissioner (**OAIC**) is responsible for data protection under the Privacy Act.
- The Australian Communications and Media Authority (**ACMA**) is responsible for the protection of privacy in accordance with the DNCR Act and Spam Act.
- The Australian Competition and Consumer Commission (**ACCC**) is responsible for administering the CDR regime pursuant to the *Competition and Consumer Act 2010* (Cth).
- The APRA is responsible for regulating powers in accordance with CPS 231 and CPS 234.
- The Australian Attorney-General's Department has responsibilities and powers in connection with the privacy of data obtained pursuant to the *Telecommunications (Interception and Access) Act 1979* (Cth).
- The Australian Transaction Reports and Analysis Centre (**AUSTRAC**) has responsibilities and functions relating to compliance with the APPs in respect of information obtained under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth).

## 2 Definitions

**2.1 Please provide the key definitions used in the relevant legislation:**

- "**Personal Data**"
  The terminology used in the Privacy Act is "personal information", which is defined to refer to information or an opinion about an identified individual, or an individual who is reasonably identifiable:
  a. whether the information or opinion is true or not; and
  b. whether the information or opinion is recorded in a material form or not.
- "**Processing**"
  "Processing" is not used in the Privacy Act. Rather, the terminology of "use" and "disclose" are used in the APPs. According to the Australian Privacy Principles Guidelines issued by the OAIC in July 2019 (**APP Guidelines**):
  - An entity "uses" personal information when it handles and manages that information within the entity's effective control.
  - An entity "discloses" personal information when it makes it accessible or visible to others outside the entity and releases the subsequent handling of the personal information from its effective control.
- "**Controller**"
  "Controller" is not used in the Privacy Act. The relevant concept is phrased as "APP entity", which means an "agency" or "organisation".
  An "organisation" is defined in the Privacy Act as:
  - an individual;
  - a body corporate;
  - a partnership;
  - any other unincorporated association; or
  - a trust,

  that is not a small business operator, a registered political party, an agency, or an authority or prescribed instrumentality of a State or Territory.
  An "agency" is set out as a defined list which includes, for instance, the following key agencies:
  - a Minister;
  - a Department;
  - a body (whether incorporated or not), or a tribunal, established or appointed for a public purpose by or under a Commonwealth enactment, not being:
    - an incorporated company, society or association; or
    - an organisation that is registered under the *Fair Work (Registered Organisations) Act 2009* (Cth);
  - a body established or appointed by the Governor-General, or by a Minister;
  - a federal court; and
  - the Australian Federal Police.
- "**Processor**"
  "Processor" is not used in the Privacy Act. The relevant terminology is "APP entity", in relation to which please refer to the definition for "Controller" above.
- "**Data Subject**"
  The phrase "Data Subject" is not used in the Privacy Act. The Privacy Act protects the personal information of "individuals", which is defined to mean natural persons. Additionally, the CDR regime (commonly referred to as "Open Banking" and discussed further under section 6 and question 18.2 below) includes provisions regarding the definition of a "CDR consumer" where a person is identifiable from data relating to the person because of the supply of a good or service to the person or one of the person's associates. CDR consumers may be individuals or bodies corporate.
- "**Sensitive Personal Data**"
  "Sensitive information" is defined in the Privacy Act as:
  a. personal information about an individual's:
     i. racial or ethnic origin;
     ii. political opinions;
     iii. membership of a political association;
     iv. religious beliefs or affiliations;
     v. philosophical beliefs;
     vi. membership of a professional trade association;
     vii. membership of a trade union;
     viii. sexual orientation or practices; or
     ix. criminal record;
  b. health information about an individual;
  c. genetic information about an individual that is not otherwise health information;
  d. biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or
  e. biometric templates.
- "**Data Breach**"
  Under s. 26WE(2) of the Privacy Act, there is an "eligible data breach" if:
  i. there is unauthorised access to, or unauthorised disclosure of, personal information held by an entity (or loss of the information in circumstances where unauthorised access to or disclosure of the information is likely to occur); and
  ii. a reasonable person would conclude that the access, disclosure or loss is likely to result in serious harm to any of the individuals to whom the information relates.
- *Other key definitions – please specify (e.g., "Pseudonymous Data", "Direct Personal Data", "Indirect Personal Data")*
  "**Collects**": An entity collects personal information only if the entity collects the personal information for inclusion in a record or generally available publication.
  "**De-identified**": Personal information is de-identified if the information is no longer about an identifiable individual or an individual who is reasonably identifiable.
  "**Holds**": An entity holds personal information if the entity has possession or control of a record that contains the personal information.
  "**Record**": The definition of a record includes a document or an electronic or other device but excludes items such as:
  a. a generally available publication;
  b. anything kept in a library, art gallery or museum for the purposes of reference, study or exhibition;
  c. Commonwealth records in the open access period;
  d. records in the care of the National Archives of Australia;
  e. documents placed in the memorial collection of the Australian War Memorial; or
  f. letters or other articles in the course of transmission by post.

  See also other definitions in s. 6 of the Privacy Act.

## 3 Territorial Scope

**3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?**

Yes, the Privacy Act applies to businesses established in other jurisdictions provided that the APP entity or small business operator has an "Australian Link". An Australian Link arises as per s. 5B(2) of the Privacy Act if an organisation or operator is:

a. an Australian citizen;
b. a person whose continued presence in Australia is not subject to a time limitation imposed by law;
c. a partnership formed in Australia or an external Territory;
d. a trust created in Australia or an external Territory;
e. a body corporate incorporated in Australia or an external Territory; or
f. an unincorporated association that has its central management and control in Australia or an external Territory.

If not described above, an organisation or small business operator may have an Australian Link as per s. 5B(3) of the Privacy Act if:

a. the organisation or operator carries out business in Australia or an external Territory; and
b. the personal information was collected or held by the organisation or operator in Australia or an external Territory, either before or at the time of the act or practice.

## 4 Key Principles

**4.1 What are the key principles that apply to the processing of personal data?**

- **Transparency**
  APP 1 is concerned with the use of personal information in an open and transparent manner. It imposes an obligation on APP entities to implement practices, procedures and systems to ensure the organisation is APP compliant.
- **Lawful basis for processing**
  Generally, the lawful basis for the collection, use or disclosure of personal information requires an entity to have obtained the consent of the individual. APP 3 limits the collection of information to what is reasonably necessary for the entity's function(s) or activity(ies). APP 3.5 restricts APP entities to collect personal information only by lawful and fair means.
- **Purpose limitation**
  If an individual has consented to an entity's collection of the individual's personal information for a primary purpose, then the information should not be used for another purpose (**secondary purpose**) save for a few exceptions, including where the individual would reasonably expect the entity to use or disclose the information for the secondary purpose. Such secondary purpose should:
  - be related to the primary purpose; and
  - in the case of sensitive information, be directly related to the primary purpose.
- **Data minimisation**
  APP 3 stipulates that personal information must not be collected unless it is reasonably necessary for, or directly related to, one or more of the entity's functions or activities. Furthermore, APP 11 requires personal information to be destroyed/de-identified where an entity no longer requires the information for any purpose for which the information may be used or disclosed under the APPs.
- **Proportionality**
  Refer to data minimisation above. Additionally, as per APP 10, an entity must take reasonable steps to ensure the personal information that is used and disclosed is accurate, up to date, complete and relevant.
- **Retention**
  As per APP 11.2, when the entity holds personal information and its purpose for use or disclosure no longer remains, the entity holding the personal information is subsequently required to destroy or de-identify the information.
- *Other key principles – please specify*
  - **Dealing with unsolicited personal information**
    Under APP 4, if an APP entity receives unsolicited personal information, the entity must determine whether it could have solicited and collected the information under APP 3. If the entity determines that it could not have done so, then it should destroy or de-identify the information in accordance with APP 4. See also further discussion of other principles in the answers below.

## 5 Individual Rights

**5.1 What are the key rights that individuals have in relation to the processing of their personal data?**

- **Right of access to data/copies of data**
  APP 12 provides an individual the right to access their data from an entity. It further stipulates timeframes in which an entity must respond to an individual's request to access their data. However, this is not applicable to information held by a government agency that has a reason not to disclose the information or where the disclosure of such information would be a serious threat to the health or safety of others, or would cause detriment to one's privacy.
- **Right to rectification of errors**
  APP 13 permits an individual to require an entity to correct their held personal information. APP 10 stipulates that personal information held, used, and disclosed by an entity should be complete, accurate and up to date.
- **Right to deletion/right to be forgotten**
  This power is limited in Australia. APP 11.2 requires an entity to take reasonable steps to destroy or de-identify personal information if it no longer needs the personal information for any purpose for which the information may be used or disclosed under the APPs.
- **Right to object to processing**
  Essentially, the processing of personal information requires notice and consent.
  APP 2 provides that individuals must have the option of dealing anonymously or by pseudonym with an APP entity, unless the APP entity is otherwise required by law or it is impracticable for the APP entity to provide such option.
  APP 5 stipulates that an individual must be informed that their personal information is collected. Therefore, if an individual objected to their information being collected and used, they could disengage with the activity.
- **Right to restrict processing**
  While APPs 3 and 6 stipulate certain restrictions on how personal information can be dealt with, an individual has no right to restrict how their information is processed. The provision of consent for the entity to collect an individual's information relinquishes the control an individual has over their personal information.

- **Right to data portability**
  APP 12 stipulates that an individual can request a copy of personal information held by an APP entity. Additionally, individuals can have their personal data transferred from one APP entity to another.
- **Right to withdraw consent**
  An individual has the right to withdraw their consent to the use of their personal information. The individual, prior to consenting in the first instance, must be informed that they have a right to withdraw consent. Additionally, an individual must be advised of the ramifications associated with the withdrawal of their consent.
- **Right to object to marketing**
  APPs 7.2 and 7.3 stipulate that APP entities must provide individuals a simple method to request the APP entity to no longer send, and the individual to no longer receive, marketing communications.
- **Right to complain to the relevant data protection authority(ies)**
  Individuals have the right to lodge privacy complaints with the OAIC if they are concerned that their personal information has been mishandled. They may also have the right to complain to external dispute resolution schemes that may help with privacy-related complaints with respect to, for instance, financial service providers, telecommunications providers, and electricity, gas or water providers in some States of Australia.

## 6 Registration Formalities and Prior Approval

**6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?**

Generally, there is no obligation to register with or notify data protection authorities such as the OAIC. As discussed further in section 15 below, certain obligations arise when specific data breaches occur.

On an industry-specific level, under CPS 231, APRA-regulated industries (including banking, insurance and superannuation) must notify APRA if they undertake outsourcing of a material business activity (including data processing activity), either as soon as possible after undertaking a domestic outsourcing activity, or prior to entering any off-shore outsourcing arrangement.

In addition, entities in industries covered by the CDR regime (commonly referred to as "Open Banking") also have accreditation obligations. The extent of an entity's obligations with respect to its processing activities falls under the accreditation requirements set out in the CDR scheme in Part IVD, Division 3 of the *Competition and Consumer Act 2010* (Cth).

**6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?**

Accreditation under the CDR scheme is in respect of the receipt and holding of CDR data.

**6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?**

CDR accreditations are made on a per legal entity basis.

**6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?**

In industries covered by the CDR scheme (see details under question 18.2 below), the CDR accreditation requirement is mandatory for all entities that receive consumer-specific data, including foreign legal entities that are subject to the *Competition and Consumer Act 2010* (Cth).

**6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?**

When applying for CDR accreditation, the applicant must state their address for service, the goods or services the applicant wishes to offer, ownership structure, number of employees, whether the applicant holds or intends to hold designated data and their intent for how they will use the data, other licences held, how the applicant manages CDR data, and whether the applicant is a fit and proper person.

**6.6 What are the sanctions for failure to register/notify where required?**

If a person holds out a false accreditation for receiving and holding CDR data, the sanctions are:

- for a body corporate, a maximum civil penalty amount being the greater of:
  (a) $10 million;
  (b) if the relevant court can determine the value of the benefit obtained from the contravention, three times the value of that benefit; or
  (c) if the court cannot determine the value of that benefit, 10% of the body corporate's annual turnover in the year preceding the contravention; or
- for a person other than a body corporate, imprisonment of five years and/or a maximum civil penalty amount of $500,000.

**6.7 What is the fee per registration/notification (if applicable)?**

No fee is currently applicable.

**6.8 How frequently must registrations/notifications be renewed (if applicable)?**

This is not applicable in Australia.

### 6.9 Is any prior approval required from the data protection regulator?

Yes, accreditation through the ACCC is a pre-requisite to receiving or holding CDR data.

### 6.10 Can the registration/notification be completed online?

Yes; the registration can be completed online.

### 6.11 Is there a publicly available list of completed registrations/notifications?

Yes, as per s. 56CE of the *Competition and Consumer Act 2010* (Cth). At the time of writing, the public listing of accredited data recipients is available here: https://www.cdr.gov.au/find-a-provider.

### 6.12 How long does a typical registration/notification process take?

As the CDR accreditation scheme is newly operational, the process and time frame have been developing and emerging gradually.

## 7 Appointment of a Data Protection Officer

### 7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

The appointment of a Data Protection Officer, which is commonly referred to as a "privacy officer" in Australia, is optional in general.

As part of the current review of the Privacy Act, the Australian Government issued a *Privacy Act Review Issues Paper* in October 2020, inviting submissions on matters for consideration in the review. In response to this, the OAIC made a submission on 11 December 2020 which included a recommendation to amend APP 1 to require entities to appoint a privacy officer(s) and ensure that privacy officer functions are undertaken.

In respect of government agencies, the Australian Information Commissioner has issued a *Privacy (Australian Government Agencies – Governance) APP Code 2017* (**Government Agencies APP Code**) which is binding on government agencies in Australia. This requires government agencies to have a designated privacy officer at all times as part of the requirements for complying with APP 1.2.

### 7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

No sanction is applicable in general.

With respect to government agencies, failure to appoint a privacy officer as required by the Government Agencies APP Code would be a breach of that Code, which is a contravention of APP 1.2 and also an interference with the privacy of an individual under clause 26A of the Privacy Act. Please see details of the sanctions under question 16.1 below.

### 7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

Such protection is not applicable in Australia generally and not provided in the Government Agencies APP Code in respect of government agencies.

### 7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

There is no formal requirement regarding the appointment of a Data Protection Officer in general.

For government agencies, the Government Agencies APP Code provides that an agency may designate an officer as a privacy officer by reference to a position or role, including by reference to a position or role in another agency. This would permit a person in a specific position in a government agency to be designated as the privacy officer of multiple government agencies.

### 7.5 Please describe any specific qualifications for the Data Protection Officer required by law.

There is no qualification generally required by law in Australia.

In connection with government agencies, the OAIC published a *Privacy Officer Toolkit* in which it recommends a privacy officer to have:

- an in-depth understanding of the Privacy Act and the Government Agencies APP Code, and the ability to translate these requirements into practice in the agency; and
- an understanding of any other legislation that governs the way the agency handles personal information.

### 7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

There is no general requirement by law on the responsibilities of the Data Protection Officer.

In relation to best/good practice:

- The OAIC published a document entitled *Privacy management framework: enabling compliance and encouraging good practice* which provides steps the OAIC expects to be taken to meet compliance obligations under APP 1.2. In this document, the OAIC recommends a commitment to (i) appoint key roles and responsibilities for privacy management, including a senior member of staff with overall accountability for privacy, and (ii) have staff responsible for managing privacy, including a key privacy officer, who are responsible for handling internal and external privacy enquiries, complaints, and access and correction requests.
- In the OAIC's submission dated 11 December 2020 in response to the *Privacy Act Review Issues Paper* (see further details under question 7.1 above), the OAIC describes a privacy officer as the first point of contact for privacy matters within an entity who is responsible for ensuring that day-to-day operational privacy activities are undertaken.

  In respect of government agencies, the Government Agencies APP Code describes privacy officers as the

primary point of contact for advice on privacy matters in a government agency and requires government agencies to ensure that the following privacy officer functions are carried out:

(a) handling of internal and external privacy enquiries, privacy complaints, and requests for access to and correction of personal information;
(b) maintaining a record of the agency's personal information holdings;
(c) assisting with the preparation of privacy impact assessments;
(d) maintaining the agency's register of privacy impact assessments; and
(e) measuring and documenting the agency's performance against the privacy management plan at least annually.

**7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?**

This is not required in general.

For government agencies, the Government Agencies APP Code requires an agency to keep the OAIC notified in writing of the contact details for the agency's privacy officer, or if an agency has more than one privacy officer, for one of its privacy officers.

**7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?**

This is not required in Australia.

For reference in relation to this:

- APP 5 requires an APP entity that collects personal information about an individual to, as is reasonable in the circumstances, provide notice to the individual (commonly referred to as "privacy notice") including of the identity and contact details of the APP entity or otherwise ensure that the individual is aware of such details.
- APP 1 requires an APP entity to have a clearly expressed privacy policy which must contain information on how an individual may (i) access personal information about the individual that is held by the entity and seek the correction of such information, and (ii) complain about a breach of the APP and how the entity will deal with such a complaint. In connection with how these requirements may be met, the *Guide to developing an APP privacy policy* published by the OAIC mentions the example of setting out in a privacy policy the relevant contact details which may include the position of the contact person, a generic telephone number, the postal address and a generic email address. An APP entity is required to take such steps as are reasonable in the circumstances to make its privacy policy available. This is usually achieved by an APP entity making its privacy policy available on its website.

## 8 Appointment of Processors

**8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?**

A business has an obligation to protect personal information under the Australian legal framework. As part of this obligation, the business is required to ensure that other entities to which it discloses personal information also comply with the relevant legal requirements. The business's obligations are more stringent for cross-border disclosure. It would be good practice for such obligations to be agreed in writing between the business and the data processor as a contractual arrangement.

For the banking, insurance and superannuation industries, APRA-regulated entities are required by CPS 234 to evaluate the design of a data processor's information security controls that protects the entities' information assets. CPS 231 also sets out requirements for these entities' outsourcing of material business activities to be documented in a binding agreement.

**8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?**

Entering agreements will always remain best practice, covering the type of personal information and purpose for its disclosure, the complaints handling process, compliance with the APPs and the implementation of a data breach response plan.

In respect of CPS 231, if an entity outsources data processing for a material business activity, the outsourcing arrangement must be contained in a written legally binding agreement signed by all parties before the outsourcing arrangement commences. CPS 231 sets out the minimum matters that must be addressed by the outsourcing agreement including, for instance:

- the form in which data is to be kept and clear provisions identifying ownership and control of data;
- confidentiality, privacy and security of information;
- offshoring arrangements (if any); and
- an indemnity to the effect that any sub-contracting by a third-party service provider of the outsourced function will be the responsibility of the third-party service provider, including liability for any failure on the part of the sub-contractor.

## 9 Marketing

**9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).**

Under APP 7, an organisation is prohibited from using or disclosing personal information for the purpose of direct marketing. However, it may do so where (in summary):

- the personal information has been directly collected from an individual in a manner reasonably expected to be used for direct marketing; or
- the personal information has been collected from a third party, or from an individual who would not reasonably expect their personal information to be used for direct marketing, and either the individual has consented to the direct marketing or it is impracticable to obtain that consent; and
- the organisation provides a simple means by which the individual may easily "opt out" of such direct marketing in each direct marketing communication and the individual has not so opted out.

Under the Spam Act, express or inferred consent is required for the sending of an electronic message.

**9.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?**

APP 7.1 encompasses not only the regulation of personal information for direct marketing but also its "disclosure" for this purpose. Therefore, this would cover business-to-business contexts where one business transfers personal information it has collected to another, and that business conducts direct marketing.

Further, APPs 7.6 and 7.7 outline the requirements related to individuals requesting not to receive direct marketing communications, including situations where the use or disclosure of their personal information is "for the purpose of facilitating direct marketing by other organisations".

**9.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).**

The DNCR Act prohibits unsolicited telemarketing calls and fax messages to numbers on the national Do Not Call Register, unless consent is obtained from the person or organisation being contacted.

The Spam Act prohibits the sending of unsolicited and non-consensual electronic messages. However, electronic messages by government bodies, political parties and charities may be exempt from this prohibition.

**9.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?**

As per s. 7 of the Spam Act, the sending of commercial electronic messages with an "Australian Link" are regulated by the Spam Act. This includes messages that:

- originate in Australia;
- are sent by an individual or organisation who is physically present in Australia, or whose central management is in Australia, at the time of sending;
- have been accessed by a computer, server or device located in Australia;
- are connected to an account-holder that is present in Australia when the message is accessed; or
- if unable to be delivered because the relevant electronic address does not exist, would have been reasonably likely to have been accessed using a computer, server or device located in Australia, had the address existed.

The DNCR Act covers telephone calls and fax messages sent to "an Australian number". This is defined as a number that is specified in the numbering scheme referred to in s. 454A of the *Telecommunications Act 1997* (Cth) or in the numbering plan referred to in s. 455 of the *Telecommunications Act 1997* (Cth) which is for use in connection with the supply of carriage services to the public in Australia. S. 9 of the DNCR Act also expressly states that it extends to acts, omissions and matters outside Australia.

**9.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?**

Yes, the ACMA is the regulatory authority charged with enforcing the DNCR Act and Spam Act and it publishes actions it takes to enforce breaches of marketing restrictions covered by these Acts.

For instance, in March 2021, an e-marketing company was fined $310,000 for breaching the Spam Act and sending direct marketing emails without a functional unsubscribe facility. Separately, in January 2020, a telecommunication provider was fined over $150,000 for breaching the DNCR Act by making telemarketing calls to numbers on the Do Not Call Register without consent and not ending the calls when immediately asked.

**9.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?**

A marketing list may be purchased from a third party. However, it must comply with APP 7.3. This requires that the organisation who purchases the marketing list from a third party ensures that the individuals on the list have consented to marketing or, where such consent is impractical to obtain, each communication provides the recipient with a simple means to opt out.

As per APP 7.6(e), individuals may also request to be advised of the source of their personal information used or disclosed in relation to the direct marketing.

**9.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?**

The current maximum penalties as a result of court action for the infringement of the DNCR Act or the Spam Act respectively are $2.22 million per day for a body corporate and $444,000 per day for a person that is not a body corporate. Penalties under the DNCR Act and the Spam Act are civil rather than criminal penalties. The court may also make an order directing a person who has infringed the DNCR Act and/or the Spam Act to compensate a victim who has suffered loss or damage as a result of the relevant contraventions.

## 10 Cookies

**10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).**

There is no specific legal regime that covers restrictions on the use of cookies. However, where the use of cookies rises to the level of enabling identification of an individual, it will be subject to the restrictions of the APPs. As per the APP regime, websites must have privacy policies that inform its users of all cookies that collect, process and share personal information.

**10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?**

In theory, the APPs do not apply differently to different types of cookies. However, public guidance has been given by the OAIC regarding how their distinctive operations run and how individuals may subsequently change their browsing preferences in line with this.

**10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?**

To date, the OAIC and ACMA have not reported any enforcement action in relation to cookies.

**10.4 What are the maximum penalties for breaches of applicable cookie restrictions?**

This is not applicable in Australia.

## 11 Restrictions on International Data Transfers

**11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.**

Transferring personal information to jurisdictions outside Australia is governed by APP 8. APP 8.1 stipulates that a foreign recipient of personal information must comply with the APPs. However, there are exceptions to this as per APP 8.2:

a. it is reasonably believed that the recipient is subject to a law, or binding scheme, that bears overall substantial similarity to the APPs and the individual can take action to enforce such protections;
b. the entity has obtained the individual's consent to the foreign disclosure;
c. the foreign disclosure is required or authorised by Australian law;
d. a permitted general situation (such as to lessen or prevent serious health and safety risks, or to take appropriate action in relation to suspected serious misconduct) applies;
e. such disclosure is required by a government agency under an agreement to which Australia is a party; or
f. the disclosure is by a government agency and relates to foreign law enforcement activities.

For the banking, insurance and superannuation industries, CPS 231 requires APRA-regulated entities to notify the APRA prior to entering into any off-shore outsourcing arrangement of a material business activity (including data processing activity).

**11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).**

To transfer data abroad, the OAIC expects that enforceable contracts requiring compliance with the APPs are drawn up. As per s. 16C of the Privacy Act, the Australian entity is legally responsible for any breaches of the APPs by the recipient on the basis that they believe that the foreign recipient will be compliant with the APPs.

**11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.**

There are no registration requirements in relation to the transfer of personal data.

**11.4 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?**

So far, there has been no official Australian data protection authority guidance issued following this decision. However, in response to the *Privacy Act Review Issues Paper* issued by the Australian Government in October 2020, the OAIC made a submission on 11 December 2020 which included discussion of the *Schrems* decision. See further details under question 11.5 below.

**11.5 What guidance (if any) has/have the data protection authority(ies) issued in relation to the European Commission's revised Standard Contractual Clauses?**

So far, there has been no official Australian data protection authority guidance issued in this regard. However, the OAIC has made a submission on 11 December 2020 in response to the *Privacy Act Review Issues Paper* issued by the Australian Government in October 2020.

In the OAIC's submission, it highlights the importance of entities to be able to satisfy themselves that the receiving entity is able to comply with the Standard Contract Clauses in a way which provides meaningful protections. The response indicates that entities should consider the broader legal frameworks and practices that the receiving country's privacy framework is subject to in order to make an assessment as to whether the implemented safeguards provide an equivalent standard of protection, particularly placing the onus on data controllers, exporters and importers.

## 12 Whistle-blower Hotlines

**12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?**

The *Corporations Act 2001* (Cth) (**Corporations Act**) provides protections for whistle-blowers who report misconduct or an improper state of affairs or circumstances in relation to a regulated entity(ies) (including companies, banks, insurers, etc.) or its officer or employee. This includes a disclosure of information if the discloser has reasonable grounds to suspect that a regulated entity has contravened the Corporations Act, the *Australian Securities and Investments Commission Act 2001* (Cth), the *Banking Act 1959* (Cth), the *Insurance Act 1973* (Cth) and other prescribed legislation. Whistle-blowers are protected by the Corporations Act from civil, criminal or administrative liability, contractual or other remedy, contractual termination or victimisation.

In order to be protected under the Corporations Act, the discloser must be an eligible whistle-blower, which includes an individual who is or has been an officer, employee, supplier or employee of a supplier (whether paid or unpaid) or associate of a regulated entity or a relative or dependant of any of these individuals.

An eligible whistle-blower is protected under the Corporations Act if disclosure is made to the Australian Securities and Investments Commission (**ASIC**), the Australian Prudential Regulation Authority, a prescribed Commonwealth authority or eligible recipients including an officer, senior manager, auditor, actuary or any other person authorised by the regulated entity to receive such disclosures, or to a legal practitioner for the purpose of obtaining legal advice or representation relating to such protection.

Since 1 January 2020, all public companies, large proprietary companies and corporate trustees of registrable superannuation entities have been required to have a whistle-blower policy and to make it available to officers and employees of the company.

**12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?**

An eligible whistle-blower may choose to provide his or her name and contact details or report anonymously without affecting his or her eligibility for protection under the Corporations Act. With respect to anonymous reports, ASIC has noted that they will not be able to follow up with anonymous whistle-blowers for further information or steps to be taken.

Separately, the OAIC requires any person lodging a privacy complaint with them to provide his or her name and contact details as the OAIC cannot investigate an anonymous complaint.

## 13 CCTV

**13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?**

No; the use of CCTV does not require separate registration, notification or prior approval from data protection authorities.

However, public sector agencies must advise individuals that their personal information is being collected, the purpose for which the information is being collected, the intended recipients of the information, whether the supply of the information is required by law or is voluntary, the ability to access and correct the information, and the agency's details.

Australian Government agencies and organisations with an annual turnover of more than $3 million, as well as some other organisations (APP entities) must also comply with the APPs in relation to personal information, including notifying individuals that their image may be captured.

In addition, some industries, such as buses and taxis, operate under industry specific laws that regulate their use of CCTV. For instance, in the State of New South Wales, the operator of a bus or taxi service must ensure that signs are conspicuously placed within and on the outside of a bus or taxi advising persons that they may be under video surveillance.

There are also notice requirements in relation to employee surveillance. Please refer to the discussion under question 14.1 below for further information.

**13.2 Are there limits on the purposes for which CCTV data may be used?**

Yes, there are limits on the purposes for which CCTV data may be used.

For example, federal police, Commonwealth agencies and public sector agencies may only collect personal information if it is directly related to a function or activity of the agency.

These agencies, as well as APP entities, must not use the personal information for a purpose other than that for which it was collected, unless certain exemptions apply, such as the individual having consented to the use of the information.

## 14 Employee Monitoring

**14.1 What types of employee monitoring are permitted (if any), and in what circumstances?**

The monitoring of employees is regulated at the state level. New South Wales, Victoria and the Australian Capital Territory have specific legislation regulating workplace surveillance. The other States and the Northern Territory rely on general surveillance legislation.

In the State of New South Wales, for example, employees can be monitored by:

(a) camera surveillance, which is surveillance by means of a camera that monitors or records visual images;
(b) computer surveillance, which is surveillance by means of software or other equipment that monitors or records the information input or output, or other use, of a computer; and
(c) tracking surveillance, which is surveillance by means of an electronic device to monitor or record geographical location or movement.

These types of employee monitoring can be used while the employee is at work for the employer. "At work" is defined as at a workplace of the employer (or a related corporation of the employer), regardless of whether the employee is actually performing work at the time, or at any other place while performing work for the employer (or a related corporation of the employer).

Surveillance of changing rooms and bathrooms is prohibited.

**14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.**

Yes; consent or notice is generally required. The requirements for consent or notice differ per State.

In New South Wales, for example:

(a) employees must be notified at least 14 days before the surveillance commences (or before a new employee commences work if they are due to commence within 14 days). This notice can be sent by email;
(b) the notice must indicate the kind of surveillance to be carried out, how it will be carried out, when it will start, whether it will be continuous or intermittent, and whether it will be for a specified limited period or ongoing;
(c) in relation to camera surveillance, signage must be erected that is clearly visible at each entrance notifying employees that they may be under surveillance;
(d) in relation to computer surveillance, employees must be notified of the employer's policy on computer surveillance; and

(e) in relation to tracking surveillance, a notice must be clearly visible on the vehicle indicating that the vehicle is the subject of tracking surveillance.

**14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?**

There is no requirement for works councils, trade unions or employee representatives to be notified or consulted.

## 15 Data Security and Data Breach

**15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?**

The Privacy Act does not distinguish between data controllers and data processors. All entities (to which the Privacy Act applies) are subject to the same obligations. The Privacy Act applies to Australian Government agencies and organisations with an annual turnover of more than $3 million, as well as some other organisations (APP entities).

APP 11 requires all APP entities to take reasonable steps to protect personal information they hold from misuse, interference, loss, unauthorised access, modification or disclosure.

**15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

Yes; the Privacy Act requires entities to give a notification if they have reasonable grounds to believe that an eligible data breach has happened, or it is directed to do so by the Commissioner.

If it is not clear whether the circumstances amount to an eligible data breach, the entity must carry out an assessment and take all reasonable steps to ensure that the assessment is completed within 30 days.

The entity must prepare a statement that sets out the identity and contact details of the entity, a description of the eligible data breach, the kinds of information concerned, and recommendations of the steps that individuals should take in response. The entity must give a copy of this statement to the Commissioner as soon as practicable.

For the banking, insurance and superannuation sector, CPS 234 requires APRA-regulated entities to notify APRA as soon as possible, and in any case no later than 72 hours after becoming aware of an information security incident. An APRA-regulated entity must also notify APRA as soon as possible, and in any case no later than 10 business days, after it becomes aware of a material information security control weakness which the entity expects it will not be able to remediate in a timely manner. An APRA-regulated entity includes an authorised deposit-taking institution, general insurer, life company, private health insurer and RSE licensee (as that term is defined in the *Superannuation Industry (Supervision) Act 1993* (Cth) with respect to registrable superannuation entities).

**15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

Yes; the Privacy Act requires the entity, if practicable to do so, to take reasonable steps to notify the contents of the statement described above to each individual to whom the information relates or who are at risk from the eligible date breach. If not, then the entity must publish a copy of the statement on the entity's website (if any) and take reasonable steps to publicise the contents of the statement. The entity must do so as soon as practicable after completing the statement.

**15.4 What are the maximum penalties for data security breaches?**

The maximum penalty for data security breaches under the Privacy Act is currently $2.22 million for a body corporate.

## 16 Enforcement and Sanctions

**16.1 Describe the enforcement powers of the data protection authority(ies).**

(a) **Investigative Powers**: An investigation may be commenced by the OAIC into a suspected or alleged interference with privacy, either on receipt of a complaint or as a Commissioner-initiated investigation. The OAIC is able to investigate this if certain conditions are satisfied (ss 36, 40 of the Privacy Act) and the complaint is not declined under s. 41 or referred to an alternative complaint body under s. 50.

(b) **Corrective Powers**: Enforcement powers include powers to accept an enforceable undertaking (s. 33E); bring proceedings to enforce an enforceable undertaking (s. 33F); make a determination (s. 52); bring proceedings to enforce a determination (ss 55A and 62); report to the Minister in certain circumstances following a CII, monitoring activity or assessment (ss 30 and 32); seek an injunction including before, during or after an investigation or the exercise of another regulatory power (s. 98); and apply to the court for a civil penalty order for a breach of a civil penalty provision (s. 80W).

(c) **Authorisation and Advisory Powers**: Privacy regulatory powers that permit the OAIC to work with an entity to facilitate compliance with privacy legal obligations and best practice privacy practice, including powers to request an entity, group of entities, body or association to develop an APP code, or the Credit Reporting (**CR**) code (being a written code of practice about credit reporting), and apply to the Commissioner for the code to be registered, or for the Commissioner to develop the code and register it (ss 26E(2), 26G, 26P(1) and 26R); direct an agency (but not an organisation) to give the Commissioner a privacy impact assessment (**PIA**) (s 33D); monitor, or conduct an assessment of, whether personal information is being maintained and handled by an entity as required by law (ss 28A and 33C); and direct a regulated entity to notify individuals at risk of serious harm, as well as the Commissioner, about an eligible data breach under Part IIIC of the Privacy Act (s 26WR).

(d) **Imposition of administrative fines for infringements of specified GDPR provisions**: This is not applicable in the Australian law context.

(e) **Non-compliance with a data protection authority**: Please refer to the paragraphs above.

**16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?**

As processing activities do not generally require registration, they would not be banned unless they are in breach of applicable legislative requirements. The OAIC has the powers discussed under question 16.1 above in respect of processing activities regulated by the Privacy Act. See also further details in the last bullet point under question 5.1 above.

For banking, insurance and superannuation sectors, the APRA has regulatory powers to enforce the requirements of CPS 231 on APRA-regulated entities' data processing activities if they are material business activities outsourced by the entities.

**16.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.**

The OAIC has used its powers to approval legally binding guidelines with respect to the guidelines issued by the National Health and Medical Research Council.

Another example involves a superannuation fund in 2018 that was found by the OAIC to have unlawfully disclosed personal information of its members to third parties, ultimately ordering the superannuation fund to apologise.

Furthermore, in mid-2019, the OAIC accepted an undertaking for a company that was connected to Federal Parliament to use the information collected in relation to Parliament and subsequently contact those persons without their consent.

**16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?**

The OAIC can, and has, take(n) action on foreign organisations. An example of this occurred in 2016, where the OAIC had obtained an enforceable undertaking from a Canadian-based media company due to discomfort expressed with the security of personal information collected, as well as compliance reporting, monitoring and enforcement.

## 17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

**17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?**

Businesses are required to comply with APP 6 for any disclosure of personal information and APP 8 for cross-border disclosure of personal information. Under APP 8.1, businesses must take such steps as are reasonable in the circumstances to ensure that the foreign recipient complies with the APPs (other than APP 1) in relation to the information.

APP 8.1 does not apply to the disclosure of personal information about an individual by an APP entity to the overseas recipient if:

(a) the entity reasonably believes that:
  (i) the recipient of the information is subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way in which the APPs protect the information; and
  (ii) there are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme; or

(b) the APP entity expressly informs the individual that if he or she consents to the disclosure of the information, subclause 8.1 will not apply to the disclosure; and after being so informed, the individual consents to the disclosure.

Separately and for reference, APP 8.2 provides for an exception to permit cross-border disclosure of personal information required or authorised by or under an Australian law or a court/tribunal order but this exception does not extend to foreign law enforcement agencies.

**17.2 What guidance has/have the data protection authority(ies) issued?**

As part of the APP Guidelines, the OAIC has provided some guidance to businesses relating to disclosure to foreign law enforcement agencies in connection with APP 8.

For APP 8.2(a), the APP Guidelines mention that an overseas recipient may not be subject to a law or binding scheme where, for example:

- the overseas recipient is exempt from complying, or is authorised to not comply, with part, or all of the privacy or data protection law in the jurisdiction; or
- the recipient can opt out of the binding scheme without notice and without returning or destroying the personal information.

For APP 8.1(b), the APP Guidelines set out that the APP entity should provide the individual with a clear written or oral statement explaining the potential consequences of providing consent to the cross-border disclosure.

## 18 Trends and Developments

**18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.**

The Australian Government and the ACCC have increasingly focused on issues arising from the digital age.

In 2020, the Australian Government commenced its review of the Privacy Act and issued a *Privacy Act Review Issues Paper* in October 2020 inviting submissions on matters for consideration in the review. The period for submissions has now closed; however, there will be an opportunity to provide further feedback on a discussion paper which is scheduled for release in 2021.

This review considers whether the current enforcement system is still effective and proposes significant reform to the Privacy Act, including increasing the maximum civil penalty for serious or repeated breaches from $2.22 million to the greater of $10 million, three times the value of any benefit obtained through the misuse of information, or 10% of the entity's annual

turnover. It also contemplates the introduction of a direct right for individuals to seek redress for serious breaches of privacy.

The ACCC also appears to be committed to its 2020 compliance and enforcement priority of competition and consumer issues relating to digital platforms. In August 2020, the Federal Court ordered that a medical appointment booking app, HealthEngine, pay $2.9 million in penalties for not obtaining the informed consent of its patients to disclose their personal information. In April 2021, the Federal Court found that Google's location history settings misled consumers to believe that they could prevent their location data from being collected, when in fact, selecting "Don't save my Location History in my Google Account" alone would not have achieved this outcome.

### 18.2 What "hot topics" are currently a focus for the data protection regulator?

The long-awaited CDR regime (commonly referred to as "Open Banking") came into effect in 2020 as part of the *Competition and Consumer Act 2010* (Cth). The CDR scheme provides consumers with greater access to and control over their data, by allowing consumers to require their existing service providers (currently banks) to share consumer's data with other service providers. This is expected to increase competition and consumer choice, by permitting consumers to freely switch between service providers.

The CDR rules currently applies to consumer data relating to credit and debit cards, deposit accounts and transaction accounts, as well as data relating to mortgage and personal loans. The CDR regime will be expanding to the energy sector and possibly also the telecommunications and insurance sectors.

The CDR rules have also recently been amended to enable greater participation in the CDR regime by expanding the type of consumers to include more business customers, and improving consumer experience through greater flexibility. These changes will come into effect from 1 November 2021.

Please refer to further details discussed under section 6 above.

**Anthony Borgese** has extensive experience assisting clients in their IT, telecommunications and complex outsourcing arrangements. His practice includes domestic and cross-border outsourcing, reviewing and negotiating long-term supply and outsourcing arrangements, vendor management, cloud computing, the internet, technology disputes and cyber security.

Anthony leads the outsourcing team with over 20 years' experience of delivering strategic, commercially focused solutions within the ICT arena for client organisations. He has a solid understanding of the commercial drivers of a wide range of both public and private sector organisations and service providers.

Anthony is recognised for his expertise in leading independent guides such as *Best Lawyers* in the areas of commercial law, information technology law, outsourcing law and telecommunications law, and listed as a Leading Individual in *Chambers Asia Pacific* (TMT: IT category).

**MinterEllison**
Level 40 Governor Macquarie Tower
1 Farrer Place
Sydney NSW 2000
Australia

Tel: +61 2 9921 4250
Email: anthony.borgese@minterellison.com
URL: www.minterellison.com

MinterEllison is an international law firm, headquartered in Australia and regarded as one of the Asia-Pacific's premier law firms. Our teams collaborate across Australia, New Zealand, Asia and the UK to provide trusted, seamlessly integrated solutions to our clients.

With 267 partners and 1,183 legal staff worldwide, we understand the challenges faced by businesses operating in a globalised marketplace and offer clients services that are multi-disciplinary and industry facing. In 2017, we expanded our market-leading legal technology practice with the acquisition of ITNewcom, a top-tier technology consultancy.

MinterEllison's large and diverse client base includes blue-chip public and private companies, leading multinationals, global financial institutions, government and state-owned entities.

Our lawyers have been independently recognised amongst the world's best for their strong technical skills and ability to deliver commercially practical solutions that assist clients to achieve their business objectives.

The strength of our reputation in the technology sector was recently recognised in the 2021 Edition of *Best Lawyers* in Australia, where MinterEllison was named Law Firm of the Year for our market-leading expertise in Information Technology Law. *Best Lawyers* is well known as the oldest and most respected peer review publication in the legal profession.

**www.minterellison.com**

MinterEllison

# Belgium


Bastiaan Bruyndonckx


Olivia Santantonio


Liese Kuyken

LYDIAN

## 1 Relevant Legislation and Competent Authorities

### 1.1 What is the principal data protection legislation?

Since 25 May 2018, the principal data protection legislation in the EU has been Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (the "**General Data Protection Regulation**" or "**GDPR**"). The GDPR repealed Directive 95/46/EC (the "**Data Protection Directive**") and has led to increased (though not total) harmonisation of data protection law across the EU Member States.

### 1.2 Is there any other general legislation that impacts data protection?

The law of 13 June 2005 on electronic communications implements the requirements of Directive 2002/58/EC (as amended by Directive 2009/136/EC) (the "**ePrivacy Directive**"), which provides a specific set of privacy rules to harmonise the processing of personal data by the telecoms sector. In January 2017, the European Commission published a proposal for an ePrivacy regulation (the "**ePrivacy Regulation**") that would harmonise the applicable rules across the EU Member States and replace the current ePrivacy Directive (and its implementing national legislation). Originally, the ePrivacy Regulation was intended to apply from 25 May 2018 together with the General Data Protection Regulation. Unlike with the GDPR, however, the EU states have not yet been able to agree on the draft legislation. The last draft was published on 5 January 2021.

In addition, the Belgian legislator has adopted secondary legislation pursuant to the GDPR.

The law of 3 December 2017 on the establishment of the Data Protection Authority implements the requirements of the GDPR with respect to national supervisory authorities, and reforms the Belgian Commission for the Protection of Privacy. As of 25 May 2018, the Belgian Commission for the Protection of Privacy carries the name "**Data Protection Authority**" and has the powers and competences that the GDPR requires national supervisory authorities to possess.

A second act, the law of 30 July 2018 on the protection of individuals with respect to the processing of personal data (the "**GDPR Implementation Act**"), addresses the national substantive aspects of the GDPR and introduces several specifications and derogations, such as determining the age of consent for children in an online context and providing specific legal grounds and imposing additional security measures in relation to sensitive data. At the same time, it abolishes and replaces the 1992 Data Protection Act and the 2001 Royal Decree which implemented it.

### 1.3 Is there any sector-specific legislation that impacts data protection?

Book XII of the Code of Economic Law, which deals with certain legal aspects of information society services, provides a specific set of rules regarding the use of personal data for direct marketing purposes via electronic post, which includes email, SMS and MMS. Books VI and XIV of the Code of Economic Law, which deal with market practices and consumer protection, provide a specific set of rules regarding the use of personal data for direct marketing purposes via telephone, fax and automatic calling machines without human intervention.

The law of 3 August 2012 contains provisions relating to the processing of personal data carried out by the Federal Public Service – Finance in the framework of the carrying out of its mission.

The Flemish Decree of 18 July 2008 provides a specific set of rules concerning the exchange of administrative data by regional authorities within the Flemish region.

The Camera Act of 21 March 2007 regulates the installation and use of surveillance cameras.

As regards employee monitoring, Collective Bargaining Agreement No 68 on the use of cameras in the workplace and Collective Bargaining Agreement No 81 on the monitoring of electronic communications in the workplace are relevant.

On 8 October 2020, the Belgian legislator approved an Act prohibiting life and health insurers from processing health-sensor data. The Belgian legislator intends to prevent insurers from providing discounts on the basis of health-sensor data, even if the insurers have their policy-holders' consent.

### 1.4 What authority(ies) are responsible for data protection?

Since 25 May 2018, the former Commission for the Protection of Privacy carries the name "**Data Protection Authority**" and has the powers and competences that the GDPR requires national supervisory authorities to possess.

The "**Flemish Supervisory Commission**" was established by the Decree of 8 June 2018. As a supervisory authority, the Flemish Supervisory Commission is responsible for supervising the application of the GDPR by the Flemish administrative bodies. The competences of the Flemish Supervisory Commission are in addition, and without prejudice, to the competences of the Data Protection Authority. There are no similar authorities in the Walloon or Brussels-Capital region yet.

## 2 Definitions

### 2.1 Please provide the key definitions used in the relevant legislation:

- "**Personal Data**"
  This means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- "**Processing**"
  This means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- "**Controller**"
  This means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- "**Processor**"
  This means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
- "**Data Subject**"
  This means an individual who is the subject of the relevant personal data.
- "**Sensitive Personal Data**"
  These are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health or sex life and sexual orientation, genetic data or biometric data.
- "**Data Breach**"
  This means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
- *Other key definitions*
  "Personal Data relating to Criminal Convictions" are personal data relating to criminal convictions and offences or related security measures.

## 3 Territorial Scope

### 3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The GDPR applies to businesses that are established in any EU Member State, and that process personal data (either as a controller or processor, and regardless of whether or not the processing takes place in the EU) in the context of that establishment.

A business that is not established in any Member State but is subject to the laws of a Member State by virtue of public international law is also subject to the GDPR.

The GDPR applies to businesses outside the EU if they (either as controller or processor) process the personal data of EU residents in relation to: (i) the offering of goods or services (whether or not in return for payment) to EU residents; or (ii) the monitoring of the behaviour of EU residents (to the extent that such behaviour takes place in the EU).

## 4 Key Principles

### 4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  Personal data must be processed lawfully, fairly and in a transparent manner. Controllers must provide certain minimum information to data subjects regarding the collection and further processing of their personal data. Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
- **Lawful basis for processing**
  Processing of personal data is lawful only if, and to the extent that, it is permitted under EU data protection law. The GDPR provides an exhaustive list of legal bases on which personal data may be processed, of which the following are the most relevant for businesses: (i) prior, freely given, specific, informed and unambiguous consent of the data subject; (ii) contractual necessity (i.e., the processing is necessary for the performance of a contract to which the data subject is a party, or for the purposes of pre-contractual measures taken at the data subject's request); (iii) compliance with legal obligations (i.e., the controller has a legal obligation, under the laws of the EU or an EU Member State, to perform the relevant processing); or (iv) legitimate interests (i.e., the processing is necessary for the purposes of legitimate interests pursued by the controller, except where the controller's interests are overridden by the interests, fundamental rights or freedoms of the affected data subjects).
  It should be noted that businesses require stronger grounds to process sensitive personal data. The processing of sensitive personal data is only permitted under certain conditions, of which the most relevant for businesses are: (i) explicit consent of the data subject; (ii) the processing is necessary in the context of employment law; or (iii) the processing is necessary for the establishment, exercise or defence of legal claims.
- **Purpose limitation**
  Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed

in a manner that is incompatible with those purposes. If a controller wishes to use the relevant personal data in a manner that is incompatible with the purposes for which they were initially collected, it must: (i) inform the data subject of such new processing; and (ii) be able to rely on a lawful basis as set out above.

- **Data minimisation**
  Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed. A business should only process the personal data that it actually needs to process in order to achieve its processing purposes.
- **Proportionality**
  The processing of personal data must be balanced between the means used and the intended aim.
- **Retention**
  Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- **Data security**
  Personal data must be processed in a manner that ensures appropriate security of those data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- **Accountability**
  The controller is responsible for, and must be able to demonstrate, compliance with the data protection principles set out above.

## 5 Individual Rights

### 5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**
  A data subject has the right to obtain from the controller the following information in respect of the data subject's personal data: (i) confirmation of whether, and where, the controller is processing the data subject's personal data; (ii) information about the purposes of the processing; (iii) information about the categories of data being processed; (iv) information about the categories of recipients with whom the data may be shared; (v) information about the period for which the data will be stored (or the criteria used to determine that period); (vi) information about the existence of the rights to erasure, to rectification, to restriction of processing and to object to processing; (vii) information about the existence of the right to complain to the relevant data protection authority; (viii) where the data were not collected from the data subject, information as to the source of the data; and (ix) information about the existence of, and an explanation of the logic involved in, any automated processing that has a significant effect on the data subject.
  Additionally, the data subject may request a copy of the personal data being processed.
- **Right to rectification of errors**
  Controllers must ensure that inaccurate or incomplete data are erased or rectified. Data subjects have the right to rectification of inaccurate personal data.
- **Right to deletion/right to be forgotten**
  Data subjects have the right to erasure of their personal data (the "right to be forgotten") if: (i) the data are no longer needed for their original purpose (and no new lawful purpose exists); (ii) the lawful basis for the processing is the data subject's consent, the data subject withdraws that consent, and no other lawful ground exists; (iii) the data subject exercises the right to object, and the controller has no overriding grounds for continuing the processing; (iv) the data have been processed unlawfully; or (v) erasure is necessary for compliance with EU law or national data protection law.
- **Right to object to processing**
  Data subjects have the right to object, on grounds relating to their particular situation, to the processing of personal data where the basis for that processing is either public interest or legitimate interest of the controller. The controller must cease such processing unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the relevant data subject or requires the data in order to establish, exercise or defend legal rights.
- **Right to restrict processing**
  Data subjects have the right to restrict the processing of personal data, which means that the data may only be held by the controller, and may only be used for limited purposes if: (i) the accuracy of the data is contested (and only for as long as it takes to verify that accuracy); (ii) the processing is unlawful and the data subject requests restriction (as opposed to exercising the right to erasure); (iii) the controller no longer needs the data for their original purpose, but the data are still required by the controller to establish, exercise or defend legal rights; or (iv) verification of overriding grounds is pending, in the context of an erasure request.
- **Right to data portability**
  Data subjects have a right to receive a copy of their personal data in a commonly used machine-readable format and transfer their personal data from one controller to another or have the data transmitted directly between controllers.
- **Right to withdraw consent**
  A data subject has the right to withdraw his/her consent, freely, at any time. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject must be informed of the right to withdraw consent. It must be as easy to withdraw consent as to give it.
- **Right to object to marketing**
  Data subjects have the right to object, freely, at any time, and without justification, to the processing of personal data for the purpose of direct marketing, including profiling.
- **Right to complain to the relevant data protection authority(ies)**
  Data subjects have the right to lodge complaints concerning the processing of their personal data with the Data Protection Authority, if the data subjects live in Belgium or the alleged infringement occurred in Belgium.
- **Right to basic information**
  Data subjects have the right to be provided with information on the identity of the controller, the reasons for processing their personal data and other relevant information necessary to ensure the fair and transparent processing of personal data. This is, in principle, proactively provided by the controller at the start of collecting personal data or when entering into contact for the first time with the data subject.

## 6 Registration Formalities and Prior Approval

**6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?**

No, the obligation to notify the Data Protection Authority of any wholly or partially automated processing of personal data, which existed prior to the entry into force of the GDPR, has been abolished as of the entry into force of the GDPR on 25 May 2018.

**6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?**

This is not applicable in our jurisdiction.

**6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?**

This is not applicable in our jurisdiction.

**6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?**

This is not applicable in our jurisdiction.

**6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?**

This is not applicable in our jurisdiction.

**6.6 What are the sanctions for failure to register/notify where required?**

This is not applicable in our jurisdiction.

**6.7 What is the fee per registration/notification (if applicable)?**

This is not applicable in our jurisdiction.

**6.8 How frequently must registrations/notifications be renewed (if applicable)?**

This is not applicable in our jurisdiction.

**6.9 Is any prior approval required from the data protection regulator?**

Prior approval of the Data Protection Authority is required for transfers outside the European Economic Area (the "**EEA**") to a country not offering adequate protection of personal data and that are based upon (i) bespoke contractual safeguards rather than Standard Contractual Clauses approved by the EU Commission, (ii) Binding Corporate Rules, (iii) a code of conduct, or (iv) a certification mechanism.

**6.10 Can the registration/notification be completed online?**

This is not applicable in our jurisdiction.

**6.11 Is there a publicly available list of completed registrations/notifications?**

This is not applicable in our jurisdiction.

**6.12 How long does a typical registration/notification process take?**

This is not applicable in our jurisdiction.

## 7 Appointment of a Data Protection Officer

**7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.**

The appointment of a Data Protection Officer for controllers or processors is only mandatory in some circumstances, including where there is: (i) large-scale regular and systematic monitoring of individuals; (ii) large-scale processing of sensitive personal data; or (iii) processing carried out by a public authority or body, except in the exercise of judicial functions by courts.

The Belgian legislator has not adopted secondary legislation that renders the appointment of a Data Protection Officer mandatory in cases other than those described in the GDPR.

Where a business designates a Data Protection Officer voluntarily, the requirements of the GDPR apply as though the appointment were mandatory. In order to avoid this, it is recommended to call such person a 'Privacy Manager' or 'Privacy Responsible', for instance.

**7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?**

In the circumstances where appointment of a Data Protection Officer is mandatory, failure to comply may result in the wide range of penalties available under the GDPR.

**7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?**

The appointed Data Protection Officer should not be dismissed or penalised for performing his/her tasks and should report directly to the highest management level of the controller or processor.

**7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?**

A group of undertakings may appoint a single Data Protection

Officer provided that the Data Protection Officer is easily accessible from each establishment.

**7.5 Please describe any specific qualifications for the Data Protection Officer required by law.**

The Data Protection Officer should be appointed because of professional qualities and should have an expert knowledge of data protection law and practices. While this is not strictly defined, it is clear that the level of expertise required will depend on the circumstances. For example, the involvement of large volumes of sensitive personal data will require a higher level of knowledge.

**7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?**

The Data Protection Officer should be involved in all issues which relate to the protection of personal data. The GDPR outlines the minimum tasks required by the Data Protection Officer, which include: (i) informing the controller, processor and their relevant employees who process data of their obligations under the GDPR; (ii) monitoring compliance with the GDPR, national data protection legislation and internal policies in relation to the processing of personal data including internal audits; (iii) advising on data protection impact assessments and the training of staff; and (iv) co-operating with the Data Protection Authority and acting as the Data Protection Authority's primary contact point for issues related to data processing.

**7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?**

Yes, the controller or processor must notify the Data Protection Authority of the contact details of the designated Data Protection Officer.

**7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?**

The Data Protection Officer does not necessarily need to be named in the public-facing privacy notice. However, the contact details of the Data Protection Officer must be notified to the data subject when personal data relating to that data subject are collected. As a matter of good practice, the Article 29 Working Party (the "**WP29**") (now the European Data Protection Board (the "**EDPB**")) recommended in its 2017 guidance on Data Protection Officers that both the Data Protection Authority and employees should be notified of the name and contact details of the Data Protection Officer.

## 8 Appointment of Processors

**8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?**

Yes. The business that appoints a processor to process personal data on its behalf, is required to enter into an agreement with the processor which sets out the subject matter for processing, the duration of processing, the nature and purpose of processing, the types of personal data and categories of data subjects and the obligations and rights of the controller (i.e., the business).

It is essential that the processor appointed by the business complies with the GDPR.

**8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?**

The processor must be appointed under a binding agreement in writing. The contractual terms must stipulate that the processor: (i) only acts on the documented instructions of the controller; (ii) imposes confidentiality obligations on all employees; (iii) ensures the security of personal data that it processes; (iv) abides by the rules regarding the appointment of sub-processors; (v) implements measures to assist the controller with guaranteeing the rights of data subjects; (vi) assists the controller in obtaining approval from the relevant data protection authority; (vii) either returns or destroys the personal data at the end of the relationship (except as required by EU or Member State law); and (viii) provides the controller with all information necessary to demonstrate compliance with the GDPR, and allows for and contributes to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

## 9 Marketing

**9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).**

Direct marketing per electronic post (which includes email, SMS and MMS) is only authorised where the recipient specifically and freely consented to it (opt-in). However, there are two exceptions to this rule. Firstly, sending electronic direct marketing to legal entities using a non-personal email address (e.g., info@company.com) is allowed on an opt-out basis. Secondly, sending electronic direct marketing to existing customers about identical or similar products is also allowed on an opt-out basis, provided a number of strict conditions are met. It should be noted that, even when the recipient previously consented to the use of his/her electronic contact details for direct marketing purposes, he/she can at any time oppose the further use of his/her electronic contact details for direct marketing purposes.

**9.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?**

The restrictions apply to business-to-consumer marketing as well as in a business-to-business context.

**9.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).**

For marketing by telephone, a national opt-out register (the so-called "Do Not Call Me Robinson List") exists and businesses carrying out direct marketing by telephone are required to check this list in advance.

Direct marketing by post does not require the prior consent of the addressee but can be carried out on an opt-out basis. For direct marketing (on a personalised basis) by post, a national opt-out register has been put in place but is only mandatory for businesses that are members of the Belgian Direct Marketing Association (the "**BDMA**"). For non-personalised advertising by post, anyone can ask to be provided with "Stop-Pub" stickers to stick on his/her mailbox.

For marketing by fax or via automated calling machines without human intervention, the prior consent of the recipient is required (opt-in).

**9.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?**

Yes, they do.

**9.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?**

Under the GDPR, the Data Protection Authority will have the right to carry out investigations and enforce the GDPR, including by imposing administrative sanctions. Aside from the Data Protection Authority, the Economic Inspection (which is part of the Federal Public Service Economy) has powers to enforce the specific rules on direct marketing which form part of Books VI, XII and XIV of the Code of Economic Law. Both authorities are active in enforcement of breaches of marketing restrictions. Most investigations are, however, started on the basis of complaints filed by individuals.

**9.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?**

Yes, provided that data protection legislation is complied with. This means, amongst others, that the collection and processing of the data must have been carried out in compliance with the principles of the GDPR (including lawful basis, compliance with the opt-in and opt-out rules, transparency, purpose limitation, accuracy, security and confidentiality).

Businesses are strongly advised to seek appropriate guarantees from the seller of marketing lists, including with respect to: (i) the fact that the data have been gathered and processed in compliance with the GDPR; (ii) the fact that the individuals whose data are included have consented to the use of their data for direct marketing purposes; and (iii) the fact that the transfer of the data is in accordance with the fair processing notices provided to the individuals and with the GDPR.

**9.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?**

Based on a breach of Books VI, XII and XIV of the Code of Economic Law, in case of proceedings before Belgian criminal courts, the maximum penalty for sending marketing communications in breach of applicable restrictions is a criminal fine of EUR 10,000. This amount is to be multiplied by eight in accordance with the law on criminal surcharges. Based on a breach of GPDR, in case of proceedings before the Belgian Data Protection Authority, the maximum penalty is the higher of EUR 20,000,000 or 4% of worldwide turnover.

## 10 Cookies

**10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).**

The law of 13 June 2005 on electronic communications implements Article 5 of the ePrivacy Directive. Pursuant to Article 5 of the EU ePrivacy Directive, the storage of cookies (or other data) on an end user's device requires prior consent (the applicable standard of consent is derived from the GDPR). For consent to be valid, it must be informed, specific, freely given and must constitute a real and unambiguous indication of the individual's wishes. This does not apply if: (i) the cookie is for the sole purpose of carrying out the transmission of a communication over an electronic communications network; or (ii) the cookie is strictly necessary to provide an "information society service" (i.e., a service provided over the internet) requested by the subscriber or user, which means that it must be essential to fulfil the user's request.

The use of cookies is only authorised if the person has had, before any use of cookies, clear and precise information concerning the purpose of the processing and his/her rights. The controller must also freely give the opportunity to the subscriber or users to withdraw their consent at any time. Information must also be provided with respect to the term of validity of the cookies used.

The EU Commission intends to pass a new ePrivacy Regulation that will replace the respective national legislation in the EU Member States.

**10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?**

The applicable restrictions indeed distinguish between different types of cookies. A distinction is made, amongst others, between session cookies (which have a time limit and are deleted after the browsing session) and permanent cookies (which are kept on the user's hard drive for an indefinite duration). Furthermore, a distinction is made between first-party cookies (which are placed by the website owner) and third-party cookies (which are placed by a third party, e.g., Facebook or Google). A distinction is also made between tracking cookies (which are used to collect data about the browsing behaviour of the user on various websites) and other cookies. In principle, the storage of cookies on an end user's device requires prior consent. This does not, however, apply to merely technical cookies and necessary cookies.

**10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?**

The Belgian Institute of Postal Services and Telecommunications (the "**BIPT/IBPT**") is in charge of monitoring compliance by businesses with the law of 13 June 2005 on electronic communications, together with the Data Protection Authority. In 2017, the Commission for the Protection of Privacy (being the predecessor of the Data Protection Authority) took aim at Facebook in connection with the use of cookies for the purposes of tracking internet users and instituted proceedings against Facebook in connection therewith. By a decision dated 16 February 2018, Facebook was condemned by the Brussels Court of First Instance for having tracked an internet user without them either knowing or consenting. The court issued a fine of EUR 250,000 per day with a maximum fine of EUR 100,000,000.

In addition, recently, the Belgian Data Protection Authority imposed an administrative fine of EUR 15,000 on a company that manages a website with legal news and information, as the company did not comply with the provisions of the GDPR and the provisions of the ePrivacy Directive.

**10.4 What are the maximum penalties for breaches of applicable cookie restrictions?**

There are no specific (criminal) sanctions linked to the breach of the applicable cookie restrictions as laid down in the law of 13 June 2005 on electronic communications. To the extent the breach also constitutes a breach of the applicable data protection laws (e.g., the obligation to inform the data subject of the processing of personal data), the controller could, however, be sanctioned with fines applicable for breaches of the data protection laws. Indeed, based on a breach of GPDR, in case of proceedings before the Belgian Data Protection Authority, the maximum penalty is the higher of EUR 20,000,000 or 4% of worldwide turnover.

## 11 Restrictions on International Data Transfers

**11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.**

Data transfers to other jurisdictions that are not within the EEA can only take place if the transfer is to an "Adequate Jurisdiction" (as specified by the EU Commission), the business has implemented one of the required safeguards as specified by the GDPR, or one of the derogations specified in the GDPR applies to the relevant transfer. The EDPB Guidelines (2/2018) set out that a "layered approach" should be taken with respect to these transfer mechanisms. If the transfer is not to an Adequate Jurisdiction, the data exporter should first explore the possibility of implementing one of the safeguards provided for in the GDPR before relying on a derogation.

**11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).**

Under the GDPR, transfers are only allowed to countries that provide an adequate level of protection, or under one of the other provisions of Chapter 5 of the GDPR.

The EU Commission has compiled a list of third countries that are deemed to offer an adequate level of protection such as Andorra, Argentina, Canada, Japan, and Switzerland. Since the recent *Schrems II* Decision of the Court of Justice, the United States no longer benefits from the Privacy Shield mechanism and is not considered a country offering adequate protection. On the other hand, the Court of Justice declared that examination of Decision 2010/87 on Standard Contractual Clauses ("**SCCs Decision**") in light of the Charter of Fundamental Rights (the "**Charter**") has disclosed nothing to affect the validity of that decision, but nevertheless questioned the Standard Contractual Clauses ("**SCCs**") validity for transfers to the US and other third countries.

When transferring personal data to a country other than an Adequate Jurisdiction, businesses must ensure that there are appropriate safeguards on the data transfer, as prescribed by the GDPR. The GDPR offers a number of ways to ensure compliance for international data transfers, of which one is consent of the relevant data subject. Other common options are the use of SCCs or Binding Corporate Rules ("**BCRs**").

Businesses can adopt the Standard Contractual Clauses drafted by the EU Commission – these are available for transfers between controllers, transfers from controller to a processor or from a processor to a controller and transfers between processors. New sets of SCC have been published on 4 June 2021 by the EU Commission. Moreover, based on the *Schrems II* Decision, organisations needed to re-evaluate their data transfers to third countries if based on SCCs. Whether the SCCs are still a sufficient safeguard for transfers to certain third countries will require further examination. For instance, in the US, it is hard to see how the concerns raised by the CJEU regarding the Privacy Shield would not apply when the SCCs are at issue. International data transfers may also take place on the basis of contracts agreed between the data exporter and data importer provided that they conform to the protections outlined in the GDPR, and they have prior approval by the relevant data protection authority.

International data transfers within a group of businesses can be safeguarded by the implementation of BCRs. The BCRs will always need approval from the relevant data protection authority. Most importantly, the BCRs will need to include a mechanism to ensure they are legally binding and enforced by every member in the group of businesses. Among other things, the BCRs must set out the group structure of the businesses, the proposed data transfers and their purpose, the rights of data subjects, the mechanisms that will be implemented to ensure compliance with the GDPR and the relevant complainant procedures.

**11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.**

It is likely that the international data transfer will require prior approval from the relevant data protection authority unless they have already established a GDPR-compliant mechanism as set out above for such transfers.

In any case, most of the safeguards outlined in the GDPR will need initial approval from the data protection authority, such as the establishment of BCRs. When personal data is transferred to an Adequate Jurisdiction or using Standard Contractual Clauses, prior approval from the relevant data protection authority is not required. On the contrary, international data transfers based upon BCRs, bespoke contractual clauses, codes of conduct or certification mechanisms require prior approval from the relevant data protection authority.

**11.4 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?**

The (brief) guidance of the Belgian Data Protection Authority summarises the conclusions of the Court of Justice, advises companies to consult the FAQ published by the EDPB and explains that the Belgian Data Protection Authority is investigating the consequences of *Schrems II* but has so far not published any additional guidance.

**11.5 What guidance (if any) has/have the data protection authority(ies) issued in relation to the European Commission's revised Standard Contractual Clauses?**

No guidance has been published by the Belgian Data Protection Authority in this respect.

## 12 Whistle-blower Hotlines

**12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?**

Internal whistle-blowing schemes are generally established in pursuance of a concern to implement proper corporate governance principles in the daily functioning of businesses. Whistle-blowing is designed as an additional mechanism for employees to report misconduct internally through a specific channel and supplements a business' regular information and reporting channels, such as employee representatives, line management, quality-control personnel or internal auditors who are employed precisely to report such misconduct.

The WP29 has limited its Opinion 1/2006 on the application of EU data protection rules to internal whistle-blowing schemes to the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime. The scope of corporate whistle-blower hotlines, however, does not need to be limited to any particular issues. In the Opinion, it is recommended that the business responsible for the whistle-blowing scheme should carefully assess whether it might be appropriate to limit the number of persons eligible for reporting alleged misconduct through the whistle-blowing scheme and whether it might be appropriate to limit the number of persons who may be reported through the scheme, in particular in the light of the seriousness of the alleged offences reported.

In 2007, the Commission for the Protection of Privacy also issued a recommendation on internal whistle-blowing schemes. The recommendation provides guidance to organisations on how to implement and operate whistle-blowing schemes in accordance with data protection law, and is largely inspired by the WP29 Opinion 1/2006 discussed above.

Moreover, the Directive (EU) 2019/1937 applies to both the private and public sectors and applies to anyone who reports or discloses the obtained information concerning breaches in a work-related context. (Ex-)employees, civil servants, consultants, (un)remunerated trainees, directors and shareholders are all protected when they report a breach in good faith.

The material scope of the Directive is wide. It concerns, *inter alia*, breaches on financial services and markets, money laundering, public procurement, transport safety, protection of the environment, consumer protection, public health, protection of privacy and personal data, as well as breaches relating to the internal market. The national legislation can extend this scope with a view to ensuring that there is a comprehensive and coherent whistle-blower protection framework.

Belgium has to implement this directive in national legislation by 17 December 2021.

There is currently no legislation in place, except for the banking and insurance sectors and for certain public authorities or organisations. It is not yet clear whether, and if so to what extent, Belgium will provide more protective rules.

However, by 17 December 2021, all companies with 50 or more employees in the private sector and all public sector organisations must comply with the minimum obligations of the directive. For companies with 50 to 249 employees, a Member State can still provide an exception regarding the obligation to set up internal reporting channels: this obligation can be postponed until 17 December 2023.

**12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?**

Anonymous reporting is not prohibited under EU data protection law; however, it raises problems as regards the essential requirement that personal data should only be collected fairly. In Opinion 1/2006, the WP29 considered that only identified reports should be advertised in order to satisfy this requirement. Businesses should not encourage or advertise the fact that anonymous reports may be made through a whistle-blower scheme.

An individual who intends to report to a whistle-blowing system should be aware that he/she will not suffer due to his/her action. The whistle-blower, at the time of establishing the first contact with the scheme, should be informed that his/her identity will be kept confidential at all the stages of the process, and in particular will not be disclosed to third parties, such as the incriminated person or to the employee's line management. If, despite this information, the person reporting to the scheme still wants to remain anonymous, the report will be accepted into the scheme. Whistle-blowers should be informed that their identity may need to be disclosed to the relevant people involved in any further investigation or subsequent judicial proceedings instigated as a result of any enquiry conducted by the whistle-blowing scheme.

## 13 CCTV

**13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?**

A data protection impact assessment ("**DPIA**") must be undertaken with assistance from the Data Protection Officer when there is a systematic monitoring of a publicly accessible area on a large scale. If the DPIA suggests that the processing would result in a high risk to the rights and freedoms of individuals prior to any action being taken by the controller, the controller must consult the data protection authority.

During the course of a consultation, the controller must provide information on the responsibilities of the controller and/or processors involved, the purpose of the intended processing, a copy of the DPIA, the safeguards provided by the GDPR to protect the rights and freedoms of data subjects and where applicable, the contact details of the Data Protection Officer.

If the data protection authority is of the opinion that the CCTV monitoring would infringe the GDPR, it has to provide written advice to the controller within eight weeks of the request of a consultation and can use any of its wider investigative, advisory and corrective powers outlined in the GDPR.

The Belgian legislator introduced a new administrative obligation in the Surveillance Camera Act as well as in the Police Service Act with regard to recording the use of cameras. This register forms an extensive logbook about the use of the cameras. Moreover, according to current Belgian legislation on surveillance cameras, installing CCTV in public areas is only permitted after positive advice from the communal or city council and the

chief of police, which requires a safety investigation. In addition, when installing CCTV in public areas, the controller must inform the local chief of police.

When installing CCTV, a sign must be placed to warn individuals that the area is under CCTV surveillance and to inform them of the identity and contact details of the controller.

**13.2 Are there limits on the purposes for which CCTV data may be used?**

CCTV for surveillance purposes can only be installed and used for the following purposes: (i) to prevent, record or detect offences; (ii) to prevent, record or detect disturbances; or (iii) to maintain public order.

CCTV can only be used in the workplace for the following purposes: (i) health and safety; (ii) protection of company property; (iii) surveillance of the production process; or (iv) monitoring of the work of employees. The employer must clearly and explicitly define the purposes of the CCTV system installed in the workplace.

## 14 Employee Monitoring

**14.1 What types of employee monitoring are permitted (if any), and in what circumstances?**

According to, amongst others, Collective Bargaining Agreement N° 68 (on the use of CCTV in the workplace) and Collective Bargaining Agreement N° 81 (on the monitoring of electronic communications in the workplace):

- the employer may monitor the hours worked through the use of a time registration system, but only if the employee has been informed of this use beforehand;
- the employer may consult the electronic agenda of an employee if it is necessary for the proper conduct of the business and there are no other, less intrusive, means to obtain the information;
- the employer may systematically monitor the professional telephone conversations in order to monitor the quality of the service, depending on the employee's function; call centres must always inform their employees that the conversations may be recorded and listened to;
- emails of a professional nature may be accessed by the employer in the absence of the employee, in order to ensure the continuity of service, provided the employer complies with the data protection legislation; the employer must inform the employee beforehand that such access may happen and only look at the emails which seem to be related to ongoing cases and are related to the period in which the employee was absent without the correspondent knowing it;
- monitoring of electronic communications in the workplace is permitted to the extent the data protection laws and Collective Bargaining Agreement N° 81 are complied with;
- the use of geo-localisation is permitted under strict conditions and only if there is no other, less intrusive, manner to monitor the employees; the data should not be kept longer than necessary; if the employer wishes to conduct an in-depth investigation, he must inform the employee and provide him the opportunity to be heard; and
- monitoring of employees through CCTV installed in the workplace is permitted to the extent the data protection laws and Collective Bargaining Agreement N° 68 are complied with; the employer must clearly define the purposes of such monitoring, and if it is only to monitor the employees, the use of the CCTV must be temporary.

**14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.**

Consent is not required as it would not be freely given, taking into account the imbalance of power between the employer and the employee. Fair processing notices are always required. Employers usually inform the workers of the monitoring via the Work Regulations, via a specific policy or, when it is punctual, before the monitoring activity.

**14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?**

Pursuant to Collective Bargaining Agreement N° 68 on the protection of privacy of workers with regard to CCTV in the workplace and Collective Bargaining Agreement N° 81 concerning the protection of workers' private lives in respect of the monitoring of electronic communications in the workplace, the Works Council or, in the absence of a Works Council, the Committee for Health and Safety or the employee representatives, must be informed of the use of CCTV in the workplace and the monitoring of electronic communications in the workplace.

## 15 Data Security and Data Breach

**15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?**

Yes. Personal data must be processed in a way which ensures security and safeguards against unauthorised or unlawful processing, accidental loss, destruction and damage of the data.

Both controllers and processors must ensure they have appropriate technical and organisational measures to meet the requirements of the GDPR. Depending on the security risk, this may include: the encryption of personal data; the ability to ensure the ongoing confidentiality, integrity and resilience of processing systems; an ability to restore access to data following a technical or physical incident; and a process for regularly testing and evaluating the technical and organisational measures for ensuring the security of processing.

**15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

The controller is responsible for reporting a personal data breach without undue delay (and in any case within 72 hours of first becoming aware of the breach) to the relevant data protection authority, unless the breach is unlikely to result in a risk to the rights and freedoms of the data subject(s). A processor must notify any data breach to the controller without undue delay.

The notification must include the nature of the personal data breach, including the categories and number of data subjects concerned, the name and contact details of the Data Protection Officer or relevant point of contact, the likely consequences

of the breach and the measures taken to address the breach, including attempts to mitigate possible adverse effects.

**15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

Controllers have a legal requirement to communicate the breach to the data subject, without undue delay, if the breach is likely to result in a high risk to the rights and freedoms of the data subject.

The notification must include the name and contact details of the Data Protection Officer (or point of contact), the likely consequences of the breach and any measures taken to remedy or mitigate the breach.

The controller may be exempt from notifying the data subject if the risk of harm is remote (e.g., because the affected data is encrypted), the controller has taken measures to minimise the risk of harm (e.g., suspending affected accounts) or the notification requires a disproportionate effort (e.g., a public notice of the breach).

**15.4 What are the maximum penalties for data security breaches?**

The maximum penalty is the higher of EUR 20,000,000 or 4% of worldwide turnover.

## 16 Enforcement and Sanctions

**16.1 Describe the enforcement powers of the data protection authority(ies).**

(a) **Investigative Powers**: The Data Protection Authority has wide powers to order the controller and the processor to provide any information it requires for the performance of its tasks, to conduct investigations in the form of data protection audits, to carry out reviews on certificates issued pursuant to the GDPR, to notify the controller or processor of alleged infringement of the GDPR, to access all personal data and all information necessary for the performance of controllers' or processors' tasks and access to the premises of the data including any data processing equipment.

(b) **Corrective Powers**: The Data Protection Authority has a wide range of powers, including to issue warnings or reprimands for non-compliance, to order the controller to disclose a personal data breach to the data subject, to impose a permanent or temporary ban on processing, to withdraw a certification and to impose an administrative fine (as below).

(c) **Authorisation and Advisory Powers**: The Data Protection Authority has a wide range of powers to advise the controller, accredit certification bodies and to authorise certificates, contractual clauses, administrative arrangements and binding corporate rules as outlined in the GDPR.

(d) **Imposition of administrative fines for infringements of specified GDPR provisions**: The GDPR provides for administrative fines which can be EUR 20,000,000 or up to 4% of the business's worldwide annual turnover of the proceeding financial year.

(e) **Non-compliance with a data protection authority**: The GDPR provides for administrative fines which will be EUR 20,000,000 or up to 4% of the business's worldwide annual turnover of the proceeding financial year, whichever is higher.

**16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?**

The GDPR entitles the relevant data protection authority to impose a temporary or definitive limitation, including a ban on processing. Pursuant to the law of 3 December 2017 on the establishment of the Data Protection Authority, the inspection chamber of the Data Protection Authority can order, by way of a temporary measure, the suspension, limitation or freezing of the processing under review, if the data concerned could cause damage which is serious, immediate and difficult to repair. The litigation chamber can order the temporary or definitive freezing, restriction or prohibition of the processing.

**16.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.**

Before the law of 3 December 2017 on the establishment of the Data Protection Authority, the Commission for the Protection of Privacy did not have the power to issue a ban on a particular processing activity. However, it could institute proceedings against the controller before the regular courts and tribunals in order to obtain such a ban or transfer the matter to the Public Prosecutor for criminal proceedings against the controller. In 2017, the Commission for the Protection of Privacy instituted proceedings against Facebook before the Court of First Instance in Brussels. On 16 February 2018, the Brussels Court of First Instance condemned Facebook for having tracked internet users without their knowledge or consent, and ordered the ceasing of the unlawful processing under penalty of a fine of EUR 250,000 per day with a maximum of EUR 100,000,000.

On 2 April 2019, the Data Protection Authority issued a ban on processing activities that were infringing data protection laws, which could not be rectified. The case involved the placement of cameras in the common areas of student rooms. The placement of such cameras was to be disproportionate to the objective of combatting vandalism, damage and nuisance. In other cases, it was ordered that a processing operation shall be made compliant with the GDPR.

**16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?**

The Data Protection Authority does indeed exercise its powers against businesses established in other jurisdictions. On 16 February 2018, the Brussels Court of First Instance condemned Facebook, including Facebook Ireland Limited and Facebook Inc., for having tracked internet users without their knowledge or consent. The court ordered the ceasing of the unlawful processing under the penalty of a fine of EUR 250,000 per day with a maximum of EUR 100,000,000. The judgment has, however, been appealed by Facebook and the matter will now be heard by the Court of Appeals of Brussels. The latter referred the case for a ruling to the European Court of Justice (C-645/19). The case concerns questions on the lead supervisory authority and the cooperation between authorities in cross-border

GDPR cases. The Advocate General states that the supervisory authority in the Member State where a data controller or processor (in this case Facebook) has its main EU establishment (which is Ireland for Facebook) has a general competence to start court proceedings for GDPR infringements in relation to cross-border data processing. The Advocate General emphasised the one-stop-shop nature of a 'lead' supervisory authority in cross-border data processing cases – a contrary situation meaning the coherence of the whole system would be impacted. However, such lead supervisory authority cannot be the sole enforcer of the GDPR in cross-border cases, and ought to closely cooperate with other relevant supervisory authorities. Moreover, the Advocate-General does not exclude the possibility that other national supervisory authorities can also commence proceedings in their respective Member States, if the GDPR expressly allows them to do so, for example, where national supervisory authorities:

- act outside the material scope of the GDPR;
- investigate into cross-border data processing carried out by public authorities, in the public interest, in the exercise of official authority or by controllers not established in the Union;
- adopt urgent measures; or
- intervene following the lead supervisory authority having decided not to handle a case.

In its decision of 15 June 2021, the Court of Justice considers that the GDPR authorises, under certain conditions, a non-lead supervisory authority of a Member State to exercise its power to bring any alleged infringement of the GDPR before a court of that State and to initiate or engage in legal proceedings in relation to an instance of cross-border data processing.

## 17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

### 17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Where e-discovery requests or requests for disclosure from foreign law enforcement agencies require a transfer of personal data to non-EEA countries not offering adequate protection of personal data, businesses typically either (i) agree on appropriate safeguards with the recipient (if and to the extent possible), (ii) seek the explicit consent of the data subjects for the disclosure and transfer, (iii) limit the disclosure to anonymous data, and/or (iv) provide a legal opinion from a reputable law firm to confirm that the disclosure and transfer is not permitted under applicable data protection laws.

### 17.2 What guidance has/have the data protection authority(ies) issued?

The WP29 has issued an Opinion 1/2009 on pre-trial discovery for cross-border litigation, which provides guidance to controllers subject to EU law in dealing with requests to transfer personal data to another jurisdiction for use in civil litigation. The Data Protection Authority has not issued any specific opinions on the subject, but has indicated (amongst others, in an opinion of 2008 on the SWIFT case) that it follows the opinion of the WP29.

## 18 Trends and Developments

### 18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

The Data Protection Authority's Litigation Chamber already announced a substantial number of decisions. The sanctions imposed are diverse, as are the subject matters involved. The Belgian Data Protection Authority has most definitely shown its teeth in the last years as the Litigation Chamber issued multiple fines. The highest fine was imposed on Google (EUR 600,000), other fines vary between EUR 1,000–100,000 depending on the severity of the infringements as well as the so-called 'exemplary role' of the defendant.

The most notable decisions contain the following learnings for undertakings operating in Belgium:

- undertakings should take note that, when opting for an internal Data Protection Officer, his/her position should be carefully assessed, including whether there are possible conflicts of interests and incompatibilities such as for Compliance Officers;
- undertakings should be aware that a notification of a data breach might be a trigger for the Belgian Data Protection Authority to look for other possible infringements and may therefore give rise to an in-depth inspection by the Belgian Data Protection Authority's Inspection Service;
- as regards compliance with data subject's requests, controllers should only request proof of identity where reasonable doubt exists as to the identity of the person exercising the data subject right; and
- as regards surveillance cameras, it should be noted that controllers should (i) carefully consider the purposes of the use of surveillance cameras, (ii) consider whether the placing of surveillance cameras is proportionate to such purposes, (iii) notify the placement of surveillance cameras to the police, and (iv) ensure the related processing is mentioned in their records of processing activities.

  The Litigation Chamber was somewhat tempered in its enthusiasm to sanction non-compliance controllers and processors by the Brussels Market Court, as it has already reversed a number of decisions of the Litigation Chamber.

### 18.2 What "hot topics" are currently a focus for the data protection regulator?

In the 2019–2025 Strategic Plan, the Belgian Data Protection Authority indicated that it will focus its actions on the following aspects of the GDPR:

- the role of the data protection officer, with a particular focus on companies that have appointed a data protection officer without allowing them to act in accordance with the GDPR;
- the lawfulness of data processing activities, and more particularly the (abusive) processing of personal data based on the legitimate interests legal basis; and
- data subjects' rights, specifically the scope of some of these rights.

The Data Protection Authority also has a number of social issues high on its agenda, such as photos and cameras, data protection online and sensitive data.

**Bastiaan Bruyndonckx** is a Partner in LYDIAN's Commercial & Litigation department and heads the Information & Communications Technology (ICT) practice as well as the Information Governance & Data Protection (Privacy) practice.
Bastiaan has a particular focus on information governance, privacy, data protection and cybersecurity and advises businesses on a broad range of industry sectors.
Bastiaan is a fellow of the Belgian American Educational Foundation (BAEF) and is a member of the International Association of Privacy Professionals (IAPP).
Bastiaan is a regular speaker at seminars, workshops and conferences on privacy and data protection. He also regularly publishes in international legal reviews such as Computerrecht, Privacy & Informatie, DataGuidance, Tijdschrift voor Privacy en Persoonsgegevens and Bulletin des Assurances. Bastiaan also contributed to the book *Data Protection – The Impact of the GDPR in Insurance* with a chapter regarding the new rules on consent and the processing of special categories of data under the GDPR.

**LYDIAN**
Avenue du Port 86C b113
1000 Brussels
Belgium

Tel: +32 2 787 90 93
Email: bastiaan.bruyndonckx@lydian.be
URL: www.lydian.be

**Olivia Santantonio** is counsel in LYDIAN's Information Governance & Data Protection (Privacy) practice and IP and ICT practice.
Olivia frequently advises on data protection issues regarding, *inter alia*, the obligations and liability of the data controller and data processor, the transfer of data into and out of the EU and the processing of sensitive data. She also frequently assists clients to assess their level of compliance with the new legislation, and assists them in case of data subject requests, data breaches or Data Protection Authority requests. She also specialises in global privacy issues (GDPR compliance, contracts review, etc.).
Olivia is a member of the International Association of Privacy Professionals (IAPP) and an active member of the International Association for the Protection of Intellectual Property (AIPPI).

**LYDIAN**
Avenue du Port 86C b113
1000 Brussels
Belgium

Tel: +32 2 787 90 07
Email: olivia.santantonio@lydian.be
URL: www.lydian.be

**Liese Kuyken** is an associate in Lydian's Information & Communications Technology (ICT), Information Governance & Data Protection (Privacy) and Intellectual Property practices.
She frequently assists clients in data protection matters regarding, for instance, data processing agreements, privacy and cookie policies, and data subject rights. Liese is involved in several procedures regarding the processing of personal data, before the Belgian Data Protection Authority as well as the Belgian courts. She teaches Media Law in the journalism programme at KU Leuven, where she educates students on issues such as privacy and image rights. Furthermore, Liese is a member of the International Association of Privacy Professionals (IAPP) and has published in the legal review *Tijdschrift voor Privacy en Persoonsgegevens*.

**LYDIAN**
Avenue du Port 86C b113
1000 Brussels
Belgium

Tel: +32 2 787 91 34
Email: liese.kuyken@lydian.be
URL: www.lydian.be

LYDIAN is a full-service Belgian business law firm with an Anglo-Saxon approach to practising law. Through a fine blend of transactional law expertise and litigation skills, we deliver straight to-the-point solutions that add true value.
Our Information Governance & Data Protection (Privacy) team represents clients, large and small, from all industry sectors (including technology, retail, telecommunications, healthcare and life sciences, media, energy, insurance, banks and other financial institutions, as well as printing and publishing industries), on all aspects of information governance and data protection.
Our range of services includes corporate privacy risk management, GDPR compliance, international data transfers, records management, e-discovery, (direct) marketing, e-commerce, cybersecurity and cybercrime.
We provide assistance to our clients, from legal advice to integrated consulting on corporate privacy risk management, as well as legislative strategic policy advice and legal compliance. We also litigate on behalf of clients in data protection-related matters.
We advise clients on global data protection and privacy compliance challenges, including by taking into account data protection and privacy rules on a global basis. We frequently advise clients on multi-jurisdictional data protection (privacy) compliance projects, either dealing with the local Belgian aspects or leading the project for our clients with the support of local correspondent firms advising on local law issues.
LYDIAN is one of the few independent law firms in Belgium operating outside a US/UK law firm banner. We are a popular referral choice for foreign firms seeking a high-quality law firm in Belgium with recognised skills in information governance and data protection, such as Hogan Lovells, Luther, Norton Rose Fulbright, Taylor Wessing and Willkie Farr & Gallagher.

**www.lydian.be**

# Brazil


Larissa Galimberti


Carla Rapé Nascimento


Luiza Fonseca de Araujo

Pinheiro Neto Advogados

## 1 Relevant Legislation and Competent Authorities

### 1.1 What is the principal data protection legislation?

The General Data Protection Law (Law No. 13,709) (*Lei Geral de Proteção de Dados* – known as the "LGPD") is the principal data protection legislation in Brazil. The LGPD was enacted in August 2018 and came into force on September 18, 2020 (except for the chapter on administrative penalties provided by the LGPD that will come into effect on August 2021). The LGPD was inspired by the General Data Protection Regulation (the "GDPR") and has brought about deep changes to the data protection framework in Brazil enacting a set of rules to be observed in data processing activities.

### 1.2 Is there any other general legislation that impacts data protection?

Yes; before the enactment of the LGPD, privacy was generally protected in Brazil through the Federal Constitution, the Civil Code (Law No. 10,406/2002), the Consumer Protection Code (Law No. 8,078/1990), the Brazilian Internet Law (Law No. 12,965/2014) and Decree No. 8,771/2016, which regulates the Brazilian Internet Law. In addition, the Access to Information Law (Law No. 12,527/2011) provides regulation on the access to public information in Brazil.

According to Article 5, X, of the Brazilian Federal Constitution, dated 1988, the right to privacy and the private life of individuals is considered a fundamental right and, as such, inviolable.

The Brazilian Civil Code also assures individuals with the right to seek judicial relief to prevent the continuous infringement of their privacy rights and the right to claim indemnification for all damages arising thereof.

The Consumer Protection Code provides for specific rules in connection with the formation of consumer databases. Generally speaking, the formation of databases with consumer records must be informed to consumers whose information will be collected and such records cannot contain any negative information that is more than five years old. Consumers must be granted access to information collected about them and they have the right to demand any correction deemed necessary.

The Brazilian Internet Law also provides rules that apply to application providers; for instance, they must store log information (access date and hour associated to an IP address) for six months.

### 1.3 Is there any sector-specific legislation that impacts data protection?

Yes; specific sectors also have regulations that impact data protection; for instance, the banking and health industries.

For example, entities regulated by the Central Bank of Brazil ("BCB") are subject to the Banking Secrecy Law (Supplementary Law No. 105/2001) and the Cybersecurity Regulation (Brazilian National Monetary Council Resolution No. 4,893/2021, which replaces Resolution No. 4,658 and the Central Bank Circular No. 3,909/2018).

According to the Banking Secrecy Law, financial entities must keep confidential "all of their credit and debit transactions, as well as the services rendered". The specific situations in which information may be disclosed without it being considered a breach of the Banking Secrecy Law are listed in Article 1, paragraph 3, for example: (i) exchange of information between financial entities or ancillary entities for credit protection; (ii) disclosures determined by law or ordered by a competent authority; and (iii) disclosures expressly authorised by the interested parties (i.e., the client).

The Cybersecurity Regulation provides rules applicable to regulated financial institutions and payment institutions, in connection with certain local requirements for storing and processing data, such as: (i) internal cybersecurity governance requirements; (ii) requirements for hiring outsourced cloud computing services; and (iii) establishing a cybersecurity policy.

Positive Data Law (Law No. 12.414/2011), Decree No. 9,936/19 and Central Bank Resolution No. 4,737/19 all together regulate the creation and management of databases containing information on the payment record of individuals or legal entities, aimed at building a credit history.

On the other hand, entities in the health industry are subject to the Medical Ethics Code (Resolution No. 1,931/2009), which determines that health professionals must prevent from

disclosing any information they become aware of as a result of their activities, unless such disclosure is made with cause, due to a legal obligation or with the previous and express authorisation of the patient.

Additionally, Resolution No. 1,642/2002 of the Brazilian Federal Medical Council determines that companies which provide medical services (either directly or indirectly) shall observe medical secrecy obligations and cannot establish any requirements that may result in the disclosure of medical records or facts acknowledged by a health professional when performing his activities.

### 1.4 What authority(ies) are responsible for data protection?

The Brazilian National Data Protection Authority (the "ANPD") was created on December 28, 2018 through the Executive Order (MP) 869/2018, and confirmed by the Federal Law No. 13,853/2019, enacted on July 8, 2019. The ANPD is composed of five commissioners, appointed by the President of Brazil on November 6, 2020, and will be advised by a national council for the protection of personal data and privacy, composed of 23 unpaid members – 10 members from different spheres of government and 13 members divided as follows: three from civil society; three from academic institutions; three from confederations of the industry sector; two from the private sector; and two from labour/union organisations.

On December 4, 2020, the ANPD launched its website, which can be accessed in the following link (https://www.gov.br/anpd/pt-br).

However, in practice, we have seen other authorities in Brazil enforcing privacy rights through administrative procedures or lawsuits, such as the Department of Consumer Protection and Defense ("Procon") and the Public Prosecutor Office responsible for consumer rights. In addition, individual and collective lawsuits have been filed due to alleged violation of data privacy.

## 2 Definitions

### 2.1 Please provide the key definitions used in the relevant legislation:

- "**Personal Data**"
  Personal data refers to any information related to an identified or identifiable natural person (Article 5, I, of the LGPD). Name, address, phone number, tax ID number, etc. are all examples of personal data related to an identified person, by which you can easily identify the natural person it refers to.
  However, there is no criteria under the data protection legislation to determine what is an "identifiable natural person". While the ANPD does not provide for such criteria, personal data related to identifiable natural persons may be understood as data which, in conjunction with other data, permits you to identify a natural person, such as geolocation.
- "**Processing**"
  Processing of personal data includes any activity carried out with personal data. For instance, the collection, production, receipt, classification, use, access, reproduction, transmission, distribution, processing, filing, storage, elimination, information control, modification, communication, transfer, diffusion and extraction are all examples of data processing activities (Article 5, X, of the LGPD).
- "**Controller**"
  The controller is the natural person or legal entity, governed either by public or private law, which is in charge of making decisions about the processing of personal data (Article 5, VI, of the LGPD). The controller is responsible for determining the purpose of the processing and for appointing the appropriate legal basis for each process, among other obligations.
- "**Processor**"
  The processor is the natural person or legal entity, governed either by public or private law, which processes personal data on behalf of the controller and following the controller's instructions (Article 5, VII, of the LGPD).
  The processor along with the controller are the processing agents (Article 5, IX, of the LGPD).
- "**Data Subject**"
  The data subject is the natural person to whom the personal data refers to (Article 5, V, of the LGPD).
- "**Sensitive Personal Data**"
  The LGPD also determines sensitive personal data (Article 5, II, of the LGPD). This subgroup of personal data includes any information regarding a natural person's race or ethnic origin, religion, political opinion, trade union or religious, philosophical or political organisation membership, health, sex life, genetics or biometrics.
- "**Data Breach**"
  Data breach is not explicitly defined by the LGPD. However, the ANPD has published on its website that a security incident involving personal data is any confirmed or suspected adverse event related to a breach in the security of personal data, such as unauthorised, accidental or unlawful access that results in the destruction, loss, alteration, leakage or in any way inadequate or unlawful data processing, which may cause risk to data subjects' rights and freedoms.
- *Other key definitions – please specify (e.g., "Pseudonymous Data", "Direct Personal Data", "Indirect Personal Data")*
  - "**Anonymysed Data**"
    Anonymised data refers to data related to a natural person that cannot be identified considering the use of reasonable technical means available at the time of the data processing (Article 5, III, of the LGPD). For now, there is no guidance on what would be considered "reasonable technical means". Anonymised data are not subject to the LGPD.
  - "**Data Protection Officer**"
    The LGPD defines the Data Protection Officer ("DPO") as a person appointed by the controller and the processor to act as a communication channel between the controller, the data subjects and the ANPD (Article 5, VIII, of the LGPD). Although this is the definition of the DPO in the LGPD, there is a discussion regarding whether the processor must appoint a DPO, as Article 41, under Section II on DPO, provides that controllers shall designate a DPO for the personal data processing, and it is silent about the processors' obligation.
  - "**Consent**"
    The consent is a demonstration of the data subjects that they agree to the processing of their personal data for a specific purpose (Article 5, XII, of the LGPD). The consent must be free, informed and unequivocal.
  - "**Data Protection Impact Assessment**"
    Data protection impact assessment refers to the documentation drafted by the controller that contains a description of the personal data processing activities

that could result in risks to the civil liberties and to the fundamental rights, as well as measures, safeguards and mechanisms to mitigate risks (Article 5, XVII, of the LGPD).

## 3 Territorial Scope

**3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?**

The LGPD may be applicable to businesses established in other jurisdictions as it provides for extraterritorial reach. The LGPD applies to any data processing by natural person or by public or private legal person, regardless of the country where they are established or the country where data is hosted, provided one of the following requirements are fulfilled: (i) the data processing takes place within the Brazilian territory; (ii) the processing activity is intended to offer or supply goods or services or to process data of individuals located in the Brazilian territory; or (iii) the collection of personal data subjects to processing has taken place in Brazilian territory (Article 3 of the LGPD).

## 4 Key Principles

**4.1 What are the key principles that apply to the processing of personal data?**

- **Transparency**
  The transparency principle assures data subjects of clear, accurate and easily accessible information on processing activities and on the respective processing agents, with due regard for trade and industrial secrets (Article 6, VI, of the LGPD).
- **Lawful basis for processing**
  Every processing of personal data operation may only occur if in accordance with one of the hypotheses provided by Article 7 or Article 11 of the LGPD. These hypotheses are referred to as the lawful basis for processing.
- **Purpose limitation**
  The purpose principle requires personal data to be processed for legitimate, specific and express purposes duly informed to the data subject, without any subsequent processing in a manner incompatible with such purposes (Article 6, I, of the LGPD).
- **Data minimisation**
  Data minimisation is linked to the necessity principle. Personal data must be processed to the minimum extent necessary for achievement of the respective data processing purposes (Article 6, III, of the LGPD).
- **Proportionality**
  The proportionality principle relates to the necessity principle and thus also to data minimisation. Personal data must be processed using pertinent, proportional, non-excessive data. The type and amount of data processed must be in accordance with the intended purpose (Article 6, II and III, of the LGPD).
- **Retention**
  Personal data shall be eliminated at the end of their processing, within the scope and technical limits of the activities, but may be retained for the following purposes: (i) fulfilment of statutory or regulatory obligations by the controller; (ii) studies by research bodies, ensuring, whenever possible, the anonymisation of personal data; (iii) transfer to a third party, to the extent that the data processing requirements set forth in the LGPD are fulfilled; or (iv) exclusive use by the controller, provided they may not be accessed by a third party, and to the extent that the data are anonymised.
- *Other key principles – please specify*
  - **Adequacy**
    Personal data shall be processed in a manner consistent with the purposes informed to the data subject, also taking into consideration the context of such processing (Article 6, II, of the LGPD).
  - **Free Access**
    Data subjects shall be assured of the right to make easy and free-of-charge inquiries into processing mechanisms and duration, as well as the integrity of their personal data (Article 6, IV, of the LGPD).
  - **Data Quality**
    Data subjects shall be assured of accurate, clear, relevant and up-to-date data, to the extent necessary and for achievement of the purposes for which they are processed (Article 6, V, of the LGPD).
  - **Security**
    Technical and administrative measures shall be adopted to protect personal data from unauthorised access and from accidental or unlawful events of destruction, loss, change, communication or dissemination of such data (Article 6, VII, of the LGPD).
  - **Prevention**
    Preventive measures shall be adopted to avoid damage from processing of personal data (Article 6, VIII, of the LGPD).
  - **Non-discrimination**
    Personal data cannot be processed for discriminatory purposes, i.e., in an unlawful or abusive manner (Article 6, IX, of the LGPD).
  - **Liability and accountability**
    The processing agents shall evidence the adoption of effective measures capable of demonstrating unnecessary compliance with personal data protection rules, as well as the effectiveness of such measures (Article 6, X, of the LGPD).

## 5 Individual Rights

**5.1 What are the key rights that individuals have in relation to the processing of their personal data?**

- **Right of access to data/copies of data**
  Fulfilment of a request for access to personal data consists of making available or providing to the data subject his or her personal data processed by the controller (Articles 18, II, and 19 of the LGPD). This request for access can be made online or in writing by delivering the data in hard copy.
  There are two ways of responding to data access requests, depending on the request submitted by the data subject: (i) by means of a simplified statement, including a summary of the main personal data processed by the controller, provided immediately; and (ii) by means of a complete statement, which must also include the summary referred to above, indicating the origin of the data, the lack of records, the criteria adopted for data processing and its purpose, with due regard for trade and industrial secrets, provided within 15 days from the date of the request
- **Right to rectification of errors**
  Fulfilment of a request for rectification of incomplete,

inaccurate or outdated data consists of correcting any errors concerning personal data of the data subject (Article 18, III, of the LGPD).

- **Right to deletion/right to be forgotten**
  There are two hypotheses of a data subject's right to deletion in the LGPD, as follows:
  (i) The LGPD provides in Article 18, IV the data subject's right to anonymisation, blocking or erasure whenever the controller is processing his or her personal data in *an unnecessary or excessive manner or in violation of the LGPD*. Anonymising refers to the use of reasonable and available techniques by which the personal data indicated by the data subject can no longer be directly or indirectly associated with him or her.
  Blocking refers to the temporary suspension of any processing operation carried out with the personal data indicated by the data subject, keeping the data stored on the controller's database or systems, including an indication that they cannot be used for any other purposes.
  Erasing refers to removing from the controller's database or systems the personal data indicated by the data subject, regardless of the procedure being adopted.
  (ii) The LGPD provides in Article 18, VI, that when withdrawing his or her consent for the processing of personal data, the data subject may also request their erasure, with some exceptions as established by Article 16 (e.g., in case of the need to retain the information for compliance with legal or regulatory obligations).
  There is no rule on the general right to be forgotten in the LGPD.
- **Right to object to processing**
  Article 18, paragraph 2, of the LGPD provides that the data subject has the right to object to the processing of his or her personal data when based on one of the consent waiver events, in the event of *non-compliance with the law*. Fulfilment of a request for objection consists of stopping the processing of personal data of the data subject and suspending further processing activities, i.e., stopping any further use of the personal data of this data subject.
- **Right to restrict processing**
  Please see right to deletion above.
- **Right to data portability**
  Fulfilment of a request for portability of personal data to another service or product supplier consists of providing a copy of the personal data concerning a data subject to another company, excluding, however, information deemed as business secrets (Article 18, V, of the LGPD). The ANPD will regulate portability in the near future.
- **Right to withdraw consent**
  Fulfilment of a request for withdrawal of consent consists of stopping data processing carried out on the basis of the prior consent, and suspending further processing activities (Article 18, IX, of the LGPD), i.e., stopping any further use of the personal data being processed on the basis of the data subject's consent. In most cases, withdrawal of consent will result in the agreement with the data subject being terminated. The consent may be withdrawn at any time upon express notice of the data subject, via free-of-charge and easily accessible procedures.
  The withdrawal of consent, however, does not affect processing activities carried out before withdrawal, and in many cases the personal data will continue to be processed if there is another applicable legal basis – for example, events in which personal data should be maintained for compliance with legal obligations.
- **Right to object to marketing**
  The right to object to marketing is not explicitly provided by the LGPD.
- **Right to complain to the relevant data protection authority(ies)**
  The data subject has the right to file a petition to the ANPD (Article 18, paragraph 1, of the LGPD).
- *Other key rights – please specify*
  - **Right to confirmation**
    Fulfilment of a request for confirmation of processing consists only of informing the data subject of whether the company is processing his or her personal data, and nothing further (Article 18, I, of the LGPD). There are rare cases where the request is limited solely to confirmation as the data subject usually wishes to have access to his or her personal data as well.
  - **Right to be informed about the consequences in case of refusal to consent**
    When the controller uses consent as a legal basis for processing personal data, the data subject has the right to be informed about: (i) the possibility of refusing consent, where feasible; and (ii) the consequences of refusal, which will typically mean the impossibility of using a certain product or service (Article 18, VIII, of the LGPD).
  - **Right to anonymisation or blocking data processing**
    Please see right to deletion above.
  - **Right to request information about data sharing**
    Article 18, VII, of the LGPD ensures the data subject the right to know with which public and private entities the controller has shared his or her personal data.
  - **Right to request the review of automated-decision making**
    The data subject has the right to request a review of decisions solely based on automated processing of personal data that affect his or her interests, including decisions intended to define his or her personal, professional, consumption and credit profile or the traits of his or her personality (Article 20 of the LGPD). Fulfilment of a request for a review of decisions based on automated processing consists of providing clear and appropriate information concerning the criteria and procedures used for the automated decision, with due regard for trade and industrial secrets.

## 6 Registration Formalities and Prior Approval

### 6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

No, currently there is no obligation on businesses to register with or notify the ANPD in respect of processing activities.

The LGPD simply provides that controllers and processors must keep records of processing activities (Article 37); however, it does not give details on the format and information that must be contained in such records, nor does it impose obligations on registry of such records.

However, according to Article 10, paragraph 3 of the LGPD, the ANPD may request the controller to prepare a data protection impact assessment whenever the processing activity is based on the legitimate interest legal basis.

Furthermore, Article 38 of the LGPD states that the ANPD may request the controller to prepare a data protection impact assessment related to its data processing activities according to a regulation yet to be provided by the ANPD.

**6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?**

This is not applicable; please see above.

**6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?**

This is not applicable; please see above.

**6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?**

This is not applicable; please see above.

**6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?**

This is not applicable; please see above.

**6.6 What are the sanctions for failure to register/notify where required?**

This is not applicable; please see above.

**6.7 What is the fee per registration/notification (if applicable)?**

This is not applicable; please see above.

**6.8 How frequently must registrations/notifications be renewed (if applicable)?**

This is not applicable; please see above.

**6.9 Is any prior approval required from the data protection regulator?**

Currently, prior approval is not required from the data protection regulator.

**6.10 Can the registration/notification be completed online?**

This is not applicable; please see above. Currently, there is no obligation for registration/notification of processing activities in Brazil; therefore, there are no online features to enable the completion of a registration/notification.

**6.11 Is there a publicly available list of completed registrations/notifications?**

This is not applicable; please see above.

**6.12 How long does a typical registration/notification process take?**

This is not applicable; please see above.

## 7 Appointment of a Data Protection Officer

**7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.**

Currently, the appointment of a DPO is mandatory for a controller, and there is a discussion regarding whether a processor must appoint a DPO in relation to the activities it enacts only as a processor (and not as a controller).

In Article 5, VIII, of the LGPD, the DPO is defined as the person appointed by the controller *and processor* to act as a communication channel between the controller, the data subjects and the ANPD. However, Article 41 of the LGPD provides that any *controller* wishing to carry out personal data processing activities must appoint a DPO; there is no information regarding the processors' obligation.

Therefore, it is unclear from the Article whether it is mandatory for a processor to appoint a DPO – the ANPD may issue regulation on DPOs in the future. Once appointed, however, the DPO is subject to the applicable rules provided for in the LGPD.

After the appointment of the DPO, their identity and contact information should be made public, preferably on the data controller/processor website.

In addition, according to Article 41 of the LGPD, the ANPD may establish complementary rules on the definition and the duties of the DPO, including scenarios where a DPO does not need to be appointed, depending on the nature and the size of the entity or the volume of data being processed. However, such complementary rules have not been issued yet.

**7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?**

There are no specific sanctions for not appointing a DPO under the LGPD. However, as the appointment of a DPO is mandatory, if a DPO is not appointed, the failure to appoint can be interpreted as a violation of the LGPD.

Therefore, the sanctions for violation of the LGPD would apply. The violation of the LGPD may result in the following administrative penalties (in addition to civil liabilities): (i) warnings; (ii) fines up to two per cent (2%) of the revenues earned by the legal entity, group or conglomerate in Brazil in the preceding year, net of taxes, capped at 50 million Brazilian Reais (R$ 50,000,000.00) per offence; (iii) daily fines; (iv) disclosure of the offence; (v) blocking of the personal database to which the offence refers, until the processing activity is corrected; (vi) elimination of the personal data to which the offence refers; (vii) partial or total suspension of the operation of the database to which the offence refers for a maximum period of six months, extendable for the same period; (viii) suspension of the

processing of personal data to which the infringement refers for a maximum period of six months, extendable for the same period; and (ix) partial or total prohibition of the performance of any activities relating to data processing.

Those sanctions will be effective as of August 2021. However, we have seen other authorities in Brazil enforcing the LGPD through administrative procedures or lawsuits.

**7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?**

No, the LGPD does not provide for specific clauses regarding disciplinary measures or other employment consequences for the DPO. However, the absence of an express civil liability regime regarding the DPO in the LGPD does not exempt the DPO from the fulfilment of legal obligation, such as labour, contractual and civil.

The liability of the DPO will vary according to the DPO's role in the company's organisation. For example, in case the DPO is a statutory director, its liabilities would be similar of those of the managers of limited liability companies; in case the DPO is a non-statutory director, its liabilities would be limited to specific liabilities of employees; and in case the DPO is a third party hired to act as DPO, its liabilities would be those specified in the agreement.

**7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?**

The LGPD does not provide for any contrary provision. Therefore, it is currently possible for a business to appoint a single DPO to cover multiple entities. However, complementary regulation may be further issued by the ANPD.

**7.5 Please describe any specific qualifications for the Data Protection Officer required by law.**

The LGPD does not require specific requirements or certifications for the position of the DPO. However, recommendations and guidelines may be established in the future by the ANPD.

However, in order to comply with its roles, the DPO must have extensive technical, academic and professional knowledge in the field of data protection and on the processing activities carried out by the company.

**7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?**

According to the LGPD, the DPO has the following duties: (i) intermediate the communication between the company and data subjects; (ii) intermediate the communication between the company and the ANPD, and implement any relevant measures arising from such communication; (iii) educate the company's employees and contractors regarding data protection practices; and (iv) perform other attributions determined by the company or by complementary rules, not yet provided by the ANPD.

**7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?**

Currently, the appointment of a DPO does not need to be registered and/or notified to the ANPD. However, this may be subject to complementary regulation to be enacted in the future by the ANPD.

**7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?**

Article 41, paragraph 1, of the LGPD provides that the identity and contact information of the DPO must be publicly, clearly and objectively disclosed, preferably on the company's website.

## 8 Appointment of Processors

**8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?**

The LGPD does not have any requirements for businesses to enter into any form of agreement with their processors. Currently, the ANPD, as a recently formed public administration body, has neither issued any requirements nor regulated this topic.

Notwithstanding the lack of specific legal requirement, it is highly recommended for businesses to enter into agreements with their processors in order to establish the parties' compliance with the LGPD and any other data protection rules, the extent of the parties responsibilities and liabilities within the scope of their activities under contract, the measures to be taken in case of a data breach, collaboration in relation to the fulfilment of the data subject's rights, mechanisms applicable in case of cross-border data transfer, obligation to retain or delete information stored by data processors, and effects of the contract termination, among other obligations.

**8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?**

The LGPD does not provide for any requirements for businesses to enter into any form of agreement with their processors, as explained above. However, it is recommended as good practice to enter into an agreement in order to specify the scope of the services and data processing activities, the parties' compliance with the LGPD and any other data protection rules, the extent of the parties responsibilities and liabilities within the scope of their activities under contract, the measures to be taken in case of data breach, collaboration in relation to the fulfilment of data subject's rights, mechanisms applicable in case of cross-border data transfer, obligation to retain or delete information stored by data processors, and effects of the contract termination, among other obligations.

## 9 Marketing

**9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).**

Currently, there is no specific general regulation on the sending of electronic direct marketing; however, there are laws and regulations applicable to the matter: (i) the Brazilian Consumer

Protection Code; (ii) the LGPD; (iii) regulation issued by the National Telecommunications Agency ("Anatel"); and (iv) state laws for "do-not-spam".

The Brazilian Consumer Protection Code does not contain any specific provision regarding direct marketing actions; however, it establishes several obligations to the advertisers and suppliers that are applicable to such actions. Amongst other obligations, messages should have an opt-out option, to give the consumer the option to stop receiving direct marketing messages.

The LGPD requires a lawful base to process data. There are discussions regarding the lawful bases that would be applicable to such practices, mainly consent or legitimate interest would apply.

Anatel has issued regulation related to delivery of marketing via short message service ("SMS"). Anatel's rules apply in principle to mobile carriers only. Amongst other requirements, an opt-in must be obtained, an opt-out option must be offered and information must be clear and detailed.

Under the state laws for "do-not-spam", consumers are given the option to add their contacts to a "do-not-spam" list. The data subjects with contacts in that list must not be contacted with marketing content, be it phone calls, SMS and, in some cases, even email. The scope may vary with each state.

**9.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?**

Currently, there is no specific general regulation on the sending of electronic direct marketing in a business-to-business context. In any case, state laws for "do-not-spam" as provided above shall apply.

**9.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).**

Currently, there is no specific general regulation on the sending of electronic direct marketing; however, there are laws and regulations applicable to the matter that should be consulted, as provided above in more details: (i) the Brazilian Consumer Protection Code; (ii) the LGPD; (iii) regulation issued by Anatel; and (iv) state laws for "do-not-spam".

Restrictions may apply in other specific scenarios. The Brazilian Bank Federation ("FEBRABAN") and the Brazilian Bank Association ("ABBC") developed a self-regulation system for payroll-linked loans. In this system, bank clients may opt to not be contacted about payroll-linked loans.

Additionally, mechanisms such as opt-outs are recommended as good practice for business whenever the company relies on legitimate interest and not on the consent in relation to marketing activities.

**9.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?**

The above-mentioned provisions are applicable to any marketing communication made in Brazilian territory or whenever there is a consumer relationship regulated by Brazilian law. In relation to the LGPD, it clearly establishes an extraterritorial reach as provided in the answer to question 3.1 above.

**9.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?**

There is no specific authority in enforcement of the breaches of marketing restrictions. The ANPD, authorities related to consumer rights enforcement and others such as the Public Prosecutor's Office may take action depending on the case.

**9.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?**

Currently, there is no prohibition in law on the purchase of marketing lists from third parties. However, companies must comply with the LGPD's principles and obligations, including having an adequate lawful basis for such data processing.

**9.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?**

Non-compliance with the applicable laws may result in sanctions and penalties that will depend on the type of violation. In case of violation of the LGPD, specific administrative penalties are provided in Articles 52 to 54 (as detailed in the answer to question 7.2); in case of violation of the Brazilian Consumer Protection Code, penalties therein provided shall apply. Notwithstanding the foregoing, individual and collective lawsuits could be filed due to alleged violation of data privacy or consumer rights, seeking for indemnification for material and moral rights.

## 10 Cookies

**10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).**

Currently, there is no specific law or regulation regarding the use of cookies. However, as for any operation that involves the processing of personal data, it must observe the LGPD and its principles and obligations.

**10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?**

Currently, there is no specific law or regulation on the use of cookies; thus, law/regulation does not distinguish between different types of cookies.

**10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?**

The ANPD is still recent and taking form. There is no publicly available information on any investigations initiated by the ANPD to cookies-related matters.

**10.4 What are the maximum penalties for breaches of applicable cookie restrictions?**

Currently, there is no specific law or regulation on the use of

cookies. In case of violation of the LGPD, specific administrative penalties are provided in Articles 52 to 54 (as detailed in the answer to question 7.2); in case of violation of the Brazilian Consumer Protection Code, penalties therein provided shall apply. Notwithstanding the foregoing, individual and collective lawsuits could be filed due to alleged violation of data privacy or consumer rights, seeking for indemnification for material and moral rights.

## 11 Restrictions on International Data Transfers

**11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.**

The transfer of personal data to other jurisdictions is only permitted in accordance with the instances set forth by the LGPD, such as: (i) for cross-border transfers to third countries or international organisms with adequate protection on the same level as established by the LGPD; (ii) transfers that are necessary for international legal cooperation among intelligence, investigation and prosecution bodies; (iii) transfers that are necessary to protect the life or physical integrity of the data subject(s) or others; (iv) transfers authorised by the national authority; (v) transfers under international cooperation agreements; (vi) transfers that are necessary for executing or enforcing public policies or public services; (vii) transfers with the specific consent of the data subject; (viii) transfers that are necessary to comply with the requirements set out in II, V and VI of Article 7 of the law (for the fulfilment of a legal or regulatory obligation; if necessary, for the execution of a contract or preliminary procedures relating to a contract to which the data subject is a party, on the request of the data subject; or for the regular exercise of rights in the course of judicial, administrative or arbitration proceedings); and (ix) when the controller ensures safeguards through the use of specific contractual clauses, standard contractual clauses, global corporate clauses, seals, certificates or codes of conduct.

The content of the standard clauses, seals, certifications, codes of conduct and other specificities regarding cross-border transfer are yet to be issued by the national authority.

Please note that in case of federal administrative public entities, restrictions to the storage of data outside Brazil may apply.

Sectorial rules may impose requirements to the storage of data outside Brazil in the financial market, such as the cybersecurity regulation that applies to entities regulated or authorised by the BCB (Resolution No. 4,658/2018 (to be replaced by Resolution No. 4,893 on July 1, 2021) and Circular No. 3,909/2018 (to be replaced by Resolution No. 85 on August 1, 2021)).

**11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).**

While further regulation and/or guidelines as well as templates of the standard clauses are not issued by the ANPD, it is good business practice to establish contractual clauses that at least ensure that all parties involved in the processing and cross-border transfers are in compliance with applicable legal obligations provided by the LGPD.

**11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.**

Cross-border transfers do not require registration/notification or prior approval from the national authority. However, approval from the ANPD is one of the legal instances set forth by the LGPD that permits cross-border transfers.

**11.4 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?**

No official guidance has been issued by the authorities in Brazil.

**11.5 What guidance (if any) has/have the data protection authority(ies) issued in relation to the European Commission's revised Standard Contractual Clauses?**

No official guidance has been issued by the authorities in Brazil.

## 12 Whistle-blower Hotlines

**12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?**

The Anticorruption Law in Brazil (Law No. 12,846/2013) and its related Decree No. 8,420/2015 include the existence of a whistle-blower hotline as a parameter for the integrity programme of a company. The whistle-blower hotline must be open to all employees and third parties, be widely advertised, and must have protection mechanisms for the whistle-blowers in good faith. The current legislation does not specify or limit the permitted scope for the hotline.

**12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?**

Anonymous reporting is encouraged as one of the protection mechanisms, as mentioned in guidelines issued by the *Controladoria Geral da União* ("CGU").

## 13 CCTV

**13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?**

The use of CCTV currently does not require registration, notification and/or prior approval from the ANPD. However, as the use of CCTV involves the processing of personal data, the

controller must comply with the LGPD's principles and obligations and ensure all reasonable technical and administrative security measures are taken to guarantee the protection of the data, including the implementation of a privacy governance.

In addition, there are local and regional laws to guide and determine the adoption of additional procedures, such as those referring to the affixing of signs indicating the filming procedures; for example, São Paulo's Municipal Law No. 13,541/2003, which provides for the placement of a visible sign about filming environments and Decree No. 43,236/2003, which regulates such Municipal Law.

**13.2 Are there limits on the purposes for which CCTV data may be used?**

Neither the LGPD nor the ANPD have specifically regulated limits on the purposes for which CCTV data may be used. However, as any other processing activity, the use of CCTV data must follow the LGPD's principles and obligations. Therefore, the process must be: (i) for legitimate, specific and explicit purposes, of which the data subject is informed; (ii) compatible with the purpose notified to the data subject; (iii) limited to the minimum necessary for the achievement of the purpose of which the data subject is informed; (iv) clearly notified to the data subject; (v) protected against unauthorised use or access by technical and administrative measures; and (vi) conducted in such a way which prevents discrimination.

## 14 Employee Monitoring

**14.1 What types of employee monitoring are permitted (if any), and in what circumstances?**

The LGPD does not regulate employee monitoring and the ANPD, being only recently created, still has not provided any guidance or regulation regarding this subject. However, under Brazilian labour legislation, employers have the ability to determine how employees should render their services as well as behave in the workplace. This ability, which is commonly referred to as "employers' directive power", may include: (i) monitoring the company's email address provided to the employee; (ii) supervising the type of information and/or content which employees should not have access to while using media devices (e.g., private or improper material); (iii) creating and implementing general rules on how media devices should be used if owned and granted by the company to employees for the rendering of services (e.g., must not be taken home, should not be used for personal purposes, etc.); and (iv) placement of a CCTV system.

Therefore, if the monitoring activity can be justified by a legal basis provided by the LGPD and is not in violation of the law (specifically privacy rights), it may be performed by the employers. It is important to note that controllers (employers) must keep records of all personal data processing in a manner that it is able to demonstrate compliance with the LGPD, adopt technical and organisational security measures to protect personal data from unauthorised access and from accidental events or unlawful destruction, loss, modification, communication, dissemination or any other occurrence arising from improper or unlawful processing, and provide data subjects with sufficient information regarding the processing activities.

**14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.**

The consent of the employee is not required since there are other legal bases that could justify the processing activities related to employee monitoring, such as the regular exercise of rights in case of judicial, administrative or arbitral proceedings, execution of the employment agreement and legitimate interest, depending on the purposes of the processing. If the processing involves sensitive data, the adequate legal bases could be the regular exercise of rights in contracts and in case of judicial, administrative or arbitral proceedings, or ensuring fraud prevention and safety of data subjects in identification and record authentication proceedings in electronic systems, depending on the purposes of the data processing.

However, in order to comply with the LGPD principles, the data controllers (employers) must give transparency to the data subjects (employees) on the processing of their personal data. This means that the controller must inform the data subject of the personal data being processed and the purposes of such processing among other things, such as the data subjects' rights regarding these personal data.

This can be carried out through a general privacy notice providing all processing activities with employees' personal data, or through specific privacy notices according to the monitoring activity being performed; for instance, when providing employees with a company phone or computer devices.

**14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?**

Currently, there is no regulation indicating that work councils, trade unions and/or employee representatives should be notified or consulted in order for the employer to perform employee monitoring.

## 15 Data Security and Data Breach

**15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?**

Yes; the security of personal data is not only an obligation, but also a principle in the LGPD (Articles 6, VII, 46 and 50 of the LGPD). It is necessary for all parties involved in the processing of personal data (controllers and/or processors) to ensure and adopt technical and administrative measures to protect personal data from unauthorised access and from accidental or unlawful events of destruction, loss, change, communication or dissemination of such data. All the processing agents may be held liable in the event of failure to adopt the security measures set forth by law.

Sectorial rules may also apply. In the financial sector, for instance, cybersecurity regulation applies to entities regulated or authorised by the BCB (Resolution No. 4,658/2018 (to be replaced by Resolution No. 4,893 on July 1, 2021) and Circular No. 3,909/2018 (to be replaced by Resolution No. 85 on August 1, 2021)).

**15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

The LGPD determines that the controller shall communicate to the ANPD and to the data subject where a data breach that may cause relevant risk or damage to the data subjects has occurred (Article 48).

As set forth by the law, the communication shall be made within reasonable time. The specific timeframe is yet to be defined once the ANPD further regulates data breach requirements and definitions; however, the ANPD has recommended on its website to communicate a data breach within two business days.

According to the LGPD, the communication to the ANPD must include, at least: (i) the description of the type of affected personal data; (ii) the information regarding the data subjects involved; (iii) the technical and security measures used for data protection, with due regard for the trade and industrial secrets; (iv) the data breach risks; (v) the reasons for the delay, in case of failure to promptly communicate it; and (vi) the measures that were or will be taken to reverse or mitigate the effects of the injury.

Although the data breach will be regulated by the ANPD in the near future (and will be subject to public consultation), recently, the ANPD released a data breach form to communicate any breaches to it and has published on its website notes on data breaches. The form and the publication include extra information, in addition to the topics required by law. In case of a data breach, in addition to following the LGPD's provisions, it is recommended to check the ANPD's recommendations in its website.

Not only should data protection authorities be notified of data breaches, sectorial rules may impose notification to other authorities depending on the case; for instance, BCB, the Brazilian Securities Commission ("CVM"), among others.

**15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

The LGPD determines that the controller shall communicate to the national authority and to the data subject(s) the occurrence of a data breach that may cause relevant risk or damage to the data subject(s). The same provisions established in the answer to question 15.2 shall apply to communication with the data subject(s).

**15.4 What are the maximum penalties for data security breaches?**

The LGPD does not provide for specific penalties applicable to a data breach. Non-compliance with the applicable law may result in sanctions and penalties that will depend on the type of violation. In case of violation of the LGPD, specific administrative penalties are provided in Articles 52 to 54 (as detailed in the answer to question 7.2); in case of violation of the Brazilian Consumer Protection Code, penalties therein provided shall apply. Notwithstanding the foregoing, individual and collective lawsuits could be filed due to alleged violation of data privacy or consumer rights, seeking for indemnification for material and moral rights.

## 16 Enforcement and Sanctions

**16.1 Describe the enforcement powers of the data protection authority(ies).**

(a) **Investigative Powers**: The ANPD has administrative powers to apply sanctions and thus requires a proper prior investigation. The sanctions shall be applied after commencement of an administrative proceeding that gives the offender the opportunity of full defence, in a gradual, isolated or cumulative form, according to the features of the concrete case, and considering the lawful parameters and criteria.

(b) **Corrective Powers**: The ANPD has administrative powers to apply sanctions determined by the LGPD, such as: (i) warning, with indication of a deadline for the adoption of corrective actions; (ii) blocking of the personal data to which the offence refers, until the processing activity is regularised; (iii) erasure of the personal data to which the offence refers; (iv) partial suspension of the database to which the infringement refers for a maximum period of six months, extendable for the same period, until the processing is regularised by the controller; (v) suspension of the processing of personal data to which the infringement refers for a maximum period of six months, extendable for the same period; (vi) partial or total prohibition on data processing activities; and (vii) disclosure of the offence after the occurrence thereof has been duly investigated and confirmed.

(c) **Authorisation and Advisory Powers**: The national authority is responsible for the issue of technical opinions and recommendation; it is also the guaranteed decision-making autonomy.

(d) **Imposition of administrative fines for infringements of specified GDPR provisions**: Amongst the possible applicable sanctions by the ANPD in case of violation of the LGPD, there are administrative fees such as: (i) a one-off fine of up to two per cent (2%) of the revenues earned by the legal person, group or conglomerate in Brazil in the preceding year, net of taxes, capped at 50 million Brazilian Reais (R$ 50,000,000.00) per offence; and (ii) a daily fine, subject to the cap referred to above.

(e) **Non-compliance with a data protection authority**: In case of non-compliance with the ANPD's binding rules, the offender could be subject to the same sanctions described above. In addition, in case of non-compliance with the ANPD's decision, daily fines could be applicable as established by the LGPD.

**16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?**

Some of the administrative sanctions included in the LGPD provide for the suspension of the processing of personal data and partial or total prohibition on data processing activities. The application of these sanctions does not require a court order.

**16.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.**

The ANPD is still new and taking form. The authority focus is on structure and regulation at this moment.

However, the ANPD has started to investigate a few security incidents. Currently, there are no example cases imposing sanctions as the chapter of the administrative sanctions will enter into force on August 1, 2021.

**16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?**

The ANPD is still recent and taking form. The authority focus is on structure and regulation at this moment. Notwithstanding the foregoing, the ANPD, together with other Brazilian authorities, have issued recommendations to specific platforms in Brazil.

## 17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

**17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?**

The Brazilian Code of Civil Procedure does not provide for a broad discovery phase, as it occurs, for example, in the U.S. Therefore, the scope and depth of disclosure will mostly rely on a case-by-case analysis, that will take into account the facts and concrete elements of the case and the fulfilment of the basic legal requirements for the discovery. However, there are no blocking statutes in Brazilian civil procedural law expressly prohibiting the disclosure of data in connection with discovery obligations for litigation in other jurisdictions.

Nevertheless, Brazil has declared, under Article 23 of the Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters, that it will not execute letters of request (letters rogatory) issued for the purpose of obtaining pre-trial discovery of documents. In spite of that, the Superior Court of Justice has executed certain letters rogatory on pre-trial discovery under the understanding that the aforementioned declaration "is not to block the search for evidence abroad, but to prevent abuse" (CR 13559-US). Once again, a case-by-case analysis will be necessary.

**17.2 What guidance has/have the data protection authority(ies) issued?**

Currently, there is no guidance from the ANPD regarding e-discovery requests or requests for disclosure from foreign law enforcement agencies.

## 18 Trends and Developments

**18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.**

During the COVID-19 pandemic, Brazil has faced relevant data breach cases; specifically, one of the biggest data leaks to date, which involved 220 million people being affected. It is said that the data leaked include names, tax ID numbers, dates of birth, mothers' names, and financial information, among other data. The ANPD, as well as other authorities in Brazil, have been investigating this case.

**18.2 What "hot topics" are currently a focus for the data protection regulator?**

The ANPD has issued a request for future regulation in two topics: application of the LGPD to start-ups and small companies; and data breaches. In addition, the LGPD has been investigating data breach cases.

**Larissa Galimberti** acts in technology, licensing and data protection matters, with a focus on new technologies, digital platforms, sharing economy, e-commerce, software, data analytics, internet of things ("IoT"), cybersecurity, media and entertainment, advertising and agreements involving intellectual property rights.

**Pinheiro Neto Advogados**
Rua Hungria, 1100
São Paulo, SP
Brazil

Tel: +55 11 3247 8400
Email: lgalimberti@pn.com.br
URL: www.pinheironeto.com.br

**Carla Rapé Nascimento** is an associate and represents local and international clients in advisory matters, with a focus on technology, privacy and data protection and digital law matters. She holds a Bachelor's degree in Law from Pontifical Catholic University of São Paulo ("PUC-SP") and she is fluent in Portuguese and English.

**Pinheiro Neto Advogados**
Rua Hungria, 1100
São Paulo, SP
Brazil

Tel: +55 11 3247 8400
Email: cnascimento@pn.com.br
URL: www.pinheironeto.com.br

**Luiza Fonseca de Araujo** is an associate at Pinheiro Neto Advogados, where she has been working since 2019. She has experience in digital law, data protection and privacy, technological transactions and licensing, focusing on new technologies, platforms, software and contracts involving intellectual property rights, data protection and telecommunications. She holds a Bachelor's degree in Law from Fundação Getúlio Vargas ("FGV"), having graduated in December 2020, and she is fluent in Portuguese and English.

**Pinheiro Neto Advogados**
Rua Hungria, 1100
São Paulo, SP
Brazil

Tel: +55 11 3247 8400
Email: laraujo@pn.com.br
URL: www.pinheironeto.com.br

Pinheiro Neto Advogados is a Brazilian, independent and full-service firm specialising in multi-disciplinary deals, and was the first Brazilian law firm to specialise in corporate clients. Over more than 75 years, the firm has translated the Brazilian legal environment for the benefit of local and foreign clients.

With clients in almost 80 countries, the firm has grown organically, and developed a distinctive, tight-knit culture, with a low associate-to-partner ratio. Its unique, democratic governance structure promotes transparency and consensus-building among the partners. With a focus on innovation, the firm has kept its competitive edge throughout the years, and is widely hailed as a beacon of the Brazilian legal market.

**www.pinheironeto.com.br**

PINHEIRONETO
ADVOGADOS

# Canada


Lyndsay A. Wasser

Kristen Pennington

McMillan LLP


## 1 Relevant Legislation and Competent Authorities

### 1.1 What is the principal data protection legislation?

The *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 ("**PIPEDA**"), applies to the collection, use and disclosure of employee personal information ("**PI**") by federally regulated employers, as well as PI handled in the course of a Commercial Activity (as defined at question 2.1), except in provinces that have substantially similar legislation.

Three provinces have legislation of general application to the private sector, which are substantially similar to PIPEDA and apply to the collection, use and disclosure of both employee PI and non-employee PI within these provinces:

- Alberta – *Personal Information Protection Act*, SA 2003, c P-6.5 ("**Alberta PIPA**");
- British Columbia ("**B.C.**") – Personal Information Protection Act, SBC 2003, c 63 ("**B.C. PIPA**"); and
- Quebec – *Act respecting the protection of personal information in the private sector*, CQLR c P-39 ("**Quebec Act**").

Collectively, PIPEDA, Alberta PIPA, B.C. PIPA and the Quebec Act are referred to herein as the "**Principal Legislation**".

Some of the health privacy statutes described at question 2.3 below are also substantially similar to PIPEDA, and therefore apply to certain healthcare providers or institutions within those provinces instead of PIPEDA.

### 1.2 Is there any other general legislation that impacts data protection?

Yes; the provinces of B.C., Saskatchewan, Manitoba, Newfoundland and Labrador have each enacted statutory torts if a person wilfully violates the privacy of another.

The *Canadian Criminal Code*, RSC 1985, c C-46, includes various offences involving misuse of PI, including hacking, mischief, fraud, identity theft and circumventing technological protection measures.

The *Act to Promote the Efficiency and Adaptability of the Canadian Economy by Regulating Certain Activities that Discourage Reliance on Electronic Means of Carrying out Commercial Activities, and to Amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act*, SC 2010, c 23, commonly referred to as "Canada's Anti-Spam Legislation" ("**CASL**"), addresses certain matters involving the collection and use of email addresses as well as interference with computer systems.

Quebec's Act *to establish a legal framework for information technology*, CQLR c C-1.1 ("**Quebec's IT Act**"), requires that certain measures be taken to protect confidential information stored in electronic documents and format, and sets out rules governing the use, retention and transmission of electronic data, including biometric information.

Sections 35 through to 41 of Quebec's *Civil Code*, CQLR c CCQ-1991, govern an individual's right for his reputation and privacy to be respected, as well as unlawful invasions of privacy. Quebec's *Charter of Human Rights and Freedoms*, CQLR c C-12, also contains provisions related to privacy, including Section 5 (the right to respect for one's private life) and Section 46 (the right to fair and reasonable conditions of employment, which can restrict intrusions on employees' privacy).

### 1.3 Is there any sector-specific legislation that impacts data protection?

Yes; the *Privacy Act*, RSC, 1985, c P-21 ("**Privacy Act**"), applies to PI processed by federal government institutions. Each Canadian jurisdiction also has legislation that applies to PI handled by public bodies or institutions within the relevant province or territory.

Most provinces and territories have legislation that applies to the processing of personal health information by certain types of custodians, such as doctors and hospitals.

Most provinces also have consumer protection legislation, which includes provisions requiring consumer reporting agencies to ensure the accuracy of, limit the disclosure of, and give consumers access to their PI.

The federal *Bank Act*, RSC 1985, c C-44 ("**Bank Act**") provides for the protection of all registers and records required or authorised under the *Bank Act*, which includes certain customer records. Similarly, Quebec has credit union legislation which requires credit unions to keep customer information confidential and secure.

Some industry regulators or associations have issued guidance and/or established regulatory requirements relating to data protection, including:

- the Canadian Securities Administrators ("**CSA**");
- the Officer of the Superintendent of Financial Institutions ("**OSFI**");
- the Investment Industry Regulatory Organization ("**IIROC**"); and
- the Mutual Fund Dealers Association of Canada ("**MFDA**").

### 1.4 What authority(ies) are responsible for data protection?

Compliance with PIPEDA and the *Privacy Act* is overseen by the Office of the Privacy Commissioner of Canada ("**OPC**"), and certain offences can be prosecuted by the Attorney General.

Each province and territory also has a regulator responsible for enforcing the privacy statutes in their jurisdiction.

## 2 Definitions

### 2.1 Please provide the key definitions used in the relevant legislation:

- "**Personal Data**"
  The Principal Legislation uses the term PI, which refers to information about an identifiable individual. This has been interpreted to include any information where there is a serious possibility that an individual could be identified through the use of the information, either alone or in combination with other information.
- "**Processing**"
  This term is not defined in the Principal Legislation, which refers instead to the collection, use and disclosure of PI.
- "**Controller**"
  This term is not used in the Principal Legislation. Some obligations apply to the organisation in control of PI (e.g., breach reporting and recording requirements). An organisation is responsible for PI in its possession or custody, including information that has been transferred to a third party for processing.
- "**Processor**"
  This term is not used in the Principal Legislation. With few exceptions, the Principal Legislation generally does not distinguish between organisations that control PI and those that process PI.
- "**Data Subject**"
  This term is not used in the Principal Legislation. The Principal Legislation governs the processing of the PI of "individuals" (i.e., natural persons).
- "**Sensitive Personal Data**"
  This term is not defined in the Principal Legislation. While some categories of PI will almost always be considered sensitive (e.g., health or financial information), any PI can be considered sensitive depending on the context (taking into account the circumstances and what that information is capable of revealing when combined with other PI regarding the individual).
- "**Data Breach**"
  The equivalent term in PIPEDA is "breach of security safeguards", which refers to the loss of, unauthorised access to, or unauthorised disclosure of PI resulting from a breach of the safeguards required by PIPEDA or failure to establish such safeguards.
- *Other key definitions – please specify (e.g., "Pseudonymous Data", "Direct Personal Data", "Indirect Personal Data")*
  - "Business Contact Information" includes information that is used for the purpose of communicating or facilitating communication with an individual in relation to their employment, business or profession, such as their name, position name or title, or work address, telephone number, fax number or email. Most provisions of the Principal Legislation do not apply to Business Contact Information.
  - Under PIPEDA, "Commercial Activity" refers to a transaction, act or conduct, or any regular course of conduct, that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists.

## 3 Territorial Scope

### 3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

Yes; the Principal Legislation may apply to organisations outside of Canada in some circumstances.

For example, PIPEDA applies to foreign organisations processing PI that have a "real and substantial connection" to Canada. This is a fact-specific analysis that can take into account a variety of factors, including whether the organisation's products or services are specifically marketed to Canadians, whether the PI being processed is about Canadians, and whether any misuse or breach of PI would have an impact on Canadians (for example, by causing them distress, embarrassment or reputational harm).

## 4 Key Principles

### 4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  Organisations must make readily available to individuals, in a form that is generally understandable, specific information regarding their policies and practices with respect to PI.
- **Lawful basis for processing**
  The Principal Legislation is primarily consent-based. The knowledge and consent of the individual are required for the collection, use or disclosure of their PI, with limited exceptions. Even with consent, organisations must only collect, use and disclose PI for purposes that a reasonable person would consider appropriate in the circumstances.
- **Purpose limitation**
  At or before the time when PI is collected, organisations must generally identify and document the purposes for which such PI will be collected, used and disclosed. Subject to certain limited exceptions, PI cannot be used or disclosed for purposes other than those for which it was collected without the consent of the individual.
- **Data minimisation**
  Both the amount and type of PI must generally be limited to what is necessary for the purposes identified by the organisation when collecting the PI.
- **Proportionality**
  Organisations cannot, as a condition of supplying a product or service, require an individual to consent to the collection, use or disclosure of their PI beyond what is required to fulfil specific and legitimate purposes.
- **Retention**
  PI can generally only be retained for as long as is necessary to fulfil the purposes for which it was collected, at which point it should be destroyed, erased or made anonymous. PI that has been used to make a decision about an individual must be retained long enough to permit the individual to access the PI after the decision has been made (in B.C., at least one year).

- *Other key principles – please specify*
  - **Accountability**
    As further described at section 7 below, an organisation is responsible for PI under its control and must designate an individual or individuals who are accountable for the organisation's compliance with the Principal Legislation. Organisations must also implement certain policies and practices to give effect to their obligations under the Principal Legislation.
  - **Safeguards**
    Organisations are required to safeguard PI using reasonable physical, organisational and technological measures, which must be appropriate based on the sensitivity of the information as well as the amount, distribution, and format of the information, and the method of storage.

## 5 Individual Rights

**5.1 What are the key rights that individuals have in relation to the processing of their personal data?**

- **Right of access to data/copies of data**
  Individuals generally have the right to be informed of the existence, use and disclosure of their PI and to request access to their PI, subject to certain exceptions. Where access to PI is denied, the reasons for such denial must typically be provided.
- **Right to rectification of errors**
  If an individual successfully demonstrates that their PI is inaccurate or incomplete, the organisation usually must amend the PI and/or add a notation, as appropriate.
- **Right to deletion/right to be forgotten**
  The Principal Legislation does not currently provide for a specific right to deletion of PI or a right to be forgotten. However, giving effect to an individual's request to correct their PI and/or compliance with requirements to retain information only for the period that it is required to fulfil the purposes that it was collected may require deletion of some PI at the request of an individual.
- **Right to object to processing**
  See below regarding withdrawal of consent by an individual.
- **Right to restrict processing**
  See below regarding withdrawal of consent by an individual.
- **Right to data portability**
  The Principal Legislation does not currently provide for a right to data portability.
- **Right to withdraw consent**
  An individual can generally withdraw their consent to the collection, use and disclosure of their PI on reasonable notice, subject to legal or contractual restrictions. The organisation must inform the individual of the implications of such withdrawal.
- **Right to object to marketing**
  Under the Principal Legislation, individuals must generally consent to the collection, use and disclosure of their PI, including for marketing purposes. Use of PI for secondary purposes, including marketing purposes, must be optional (see above under "Proportionality" at question 4.1). CASL also provides that consent is required to send commercial electronic messages ("**CEM**"), and every CEM must contain an unsubscribe mechanism that can be readily performed by the individual.
- **Right to complain to the relevant data protection authority(ies)**
  Individuals have the right to file a complaint with the relevant privacy regulator(s).
- **Other key rights – please specify**
  Individuals also have a right to challenge compliance with the Principal Legislation by submitting a complaint to the organisation itself. Organisations must put in place easily accessible and simple to use procedures to receive and respond to complaints or inquiries regarding their handling of PI.

## 6 Registration Formalities and Prior Approval

**6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?**

Generally, no; however, under Quebec's IT Act, the creation or existence of a database of biometric characteristics and measurements must be disclosed to the *Commission d'accès à l'information* ("**Quebec Commission**"), whether or not the database is in service (the "**Quebec Disclosure Obligation**"). The Quebec Commission may make orders determining how such databases are to be set up, used, consulted, released and retained, and how measurements or characteristics recorded for personal identification purposes are to be archived or destroyed.

**6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?**

A mandatory form must be filed with the Quebec Commission prior to establishing the Quebec biometric information database.

**6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?**

Disclosure must be made for each Quebec biometric information database.

**6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?**

A representative of the organisation establishing the Quebec biometric information database must sign the mandatory form and attest to the truth of its contents.

**6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?**

The mandatory form that must be filed with respect to a Quebec biometric information database includes information such as the

number of people affected, the types of biometric information gathered, the objective of gathering the information, and a copy of the method of obtaining consent.

**6.6 What are the sanctions for failure to register/notify where required?**

The Quebec Commission may suspend, prohibit the bringing into service or order the destruction of a database of biometric characteristics and measurements if the database is not in compliance with the orders of the Quebec Commission or otherwise constitutes an invasion of privacy.

**6.7 What is the fee per registration/notification (if applicable)?**

There is no fee per registration/notification.

**6.8 How frequently must registrations/notifications be renewed (if applicable)?**

Provided there are no material changes to the biometric database, disclosure must only be made once per database.

**6.9 Is any prior approval required from the data protection regulator?**

As set out at question 6.1, disclosure to the Quebec Commission must be made prior to bringing the biometric database into service.

**6.10 Can the registration/notification be completed online?**

Yes; the registration/notification can be completed online.

**6.11 Is there a publicly available list of completed registrations/notifications?**

No; there is not a publicly available list of completed registrations/notifications.

**6.12 How long does a typical registration/notification process take?**

This information is not publicly available. However, the Quebec Commission recommends that the required form be submitted as early as possible to allow for sufficient processing time.

## 7 Appointment of a Data Protection Officer

**7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.**

PIPEDA, Alberta PIPA and B.C. PIPA require organisations to designate an individual or individuals to be accountable for the organisation's compliance with the legislation ("**DPO**").

**7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?**

There are currently no particular sanctions for failing to appoint a DPO. However, as set out at question 15.4, Alberta PIPA generally allows for fines where an organisation collects, uses or discloses PI in contravention of Alberta PIPA, and these fines could be applied to an organisation that fails to appoint a DPO.

**7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?**

The Principal Legislation contains anti-reprisal provisions that prohibit organisations from denying a benefit or taking adverse employment action against any employee (whether or not they are the DPO) because that employee has done or has said they will do something to avoid a contravention of the legislation.

**7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?**

Yes; a business can appoint a single DPO to cover multiple entities.

**7.5 Please describe any specific qualifications for the Data Protection Officer required by law.**

There are no statutory qualification requirements for the DPO; however, regulatory guidance indicates that they should have the support of the organisation's senior management and the authority to intervene on privacy-related issues.

**7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?**

The Principal Legislation broadly requires that the DPO is accountable for the organisation's compliance with the legislation.

*Getting Accountability Right with a Privacy Management Program* – guidance jointly published by the OPC, the Office of the Information and Privacy Commissioner of Alberta (the "**Alberta Regulator**") and the Office of the Information & Privacy Commissioner for B.C. (the "**B.C. Regulator**") – describes the DPO's responsibilities as structuring, designing and managing the organisation's privacy management programme, including all procedures, training, monitoring/auditing, documenting, evaluating, and follow-up. Other responsibilities include: establishing and implementing privacy management programme controls; coordinating with persons responsible for related discipline and functions within the organisation; ongoing assessment and revision of programme controls; representing the organisation in the event of an investigation by a regulator; and advocating about privacy within the organisation.

**7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?**

No; the appointment of a DPO does not need to be registered with or notified to the relevant data protection authority(ies).

**7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?**

PIPEDA requires that the identity of the DPO be made known upon request.

B.C. PIPA and Alberta PIPA also require that, on request, an organisation provide the name or title of the person who can answer questions regarding the organisation's collection, use, disclosure or storage of PI. Alberta PIPA also requires that this information be provided before or at the time PI is collected.

## 8 Appointment of Processors

**8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?**

An organisation that transfers PI to a third party for processing remains responsible for the PI and must use contractual or other means to protect such PI.

See section 11 below for additional considerations regarding the engagement of service providers that process PI outside of Canada.

Where applicable, public and health sector privacy legislation may also require organisations to enter into data sharing agreements with service providers.

**8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?**

The Principal Legislation does not prescribe the specific contents of a data protection agreement.

Joint guidance from the OPC, Alberta Regulator and B.C. Regulator provides that, at a minimum, agreements with service providers should include provisions that: (i) set out requirements for compliance, including binding the service provider to the policies and protocols of the organisation; (ii) require the organisation to be notified in the event of a data breach; (iii) require training and education for all service provider employees with access to PI; (iv) address subcontracting; (v) address audit rights; and (vi) require agreements with service provider employees stating that they will comply with the organisation's privacy policies and protocols.

Some industry-specific privacy laws, such as health privacy legislation, prescribe specific requirements for data protection agreements with certain service providers.

## 9 Marketing

**9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).**

In addition to being governed by the Principal Legislation, the sending of CEMs must comply with CASL in all respects. CASL requires consent to send, or cause or permit to be sent, a CEM to an electronic address. Consent must generally opt-in (upon providing certain disclosures); however there are some narrow exceptions where it may be implied for limited time periods. CASL also sets out the minimum content of CEMs, including (without limitation) the unsubscribe mechanism described at question 5.1.

**9.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?**

CASL will generally apply in a business-to-business context where CEMs are sent to electronic addresses. However, certain exceptions may apply to some business activities, for example where CEMs are sent to a person who is engaged in a commercial activity and the CEMs consist solely of an inquiry or application related to that activity.

**9.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).**

Both telephone and postal marketing must comply with the Principal Legislation in all respects.

Canada's *Unsolicited Telecommunications Rules* ("**UTR**") include additional requirements that apply to marketing by telephone. The *Telecommunications Act*, SC 1993, c 38, also establishes a National Do Not Call List ("**NDNCL**") of individuals who have registered not to receive unsolicited marketing communications by telephone or fax. Telemarketers cannot initiate, and their clients must make all reasonable efforts to ensure that they do not initiate, telemarketing telecommunications to those on the NDNCL, absent express consent.

Organisations that initiate telemarketing telecommunications on their own behalf or as a client of a telemarketer must also maintain and respect their own internal "do not call" lists.

**9.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?**

Yes; the restrictions noted above apply to marketing sent from other jurisdictions.

**9.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?**

Yes; breaches of these marketing restrictions are enforced by several regulators, including the OPC, provincial privacy regulators, the Competition Bureau and the Canadian Radio-Television and Telecommunications Commission.

**9.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?**

Organisations wishing to purchase marketing lists must ensure that individuals' meaningful consent has been obtained for the collection, use and disclosure of their PI by all relevant parties for marketing purposes.

The OPC's *Guidance for businesses doing e-marketing* recommends that, prior to purchasing or using a marketing list, organisations should ask for a detailed explanation of how: the email addresses were gathered; consent was originally obtained; the list is kept up to date; the vendor ensures that PI is promptly deleted from

the list when consent is withdrawn; and the vendor will inform the organisation of any changes to the list.

### 9.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

Persons who contravene the requirements of CASL may be subject to administrative penalties of up to $1 million for individuals and $10 million for any other person.

Persons who contravene the UTR may also be subject to penalties of up to $1,500 per violation for an individual and up to $15,000 per violation for a corporation.

See question 15.4 for a description of potential fines for organisations that collect, use or disclose PI in contravention of Alberta PIPA or the Quebec Act.

## 10 Cookies

### 10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

The OPC has taken the position that information collected about individuals' web activities by means of technologies such as cookies may constitute PI and therefore be subject to PIPEDA. Other regulators may take a similar position; therefore, the use of cookies should comply with any applicable privacy laws.

In its *Policy position on online behavioural advertising*, the OPC sets out specific considerations related to the use of online behavioural advertising ("**OBA**"), including conditions that must be satisfied in order for an organisation to rely on individuals' implied consent to the collection, use and disclosure of their non-sensitive PI for OBA. For example, individuals must be made aware of the purposes of the OBA in a clear and understandable manner at or before the time of collection and must be able to easily opt-out of the OBA with immediate and persistent effect.

Under CASL, a person is generally prohibited from installing a computer program on another person's computer system, unless they have the express consent of the other person to do so. A person is considered to consent to the installation of a computer program if the person's conduct is such that it is reasonable to believe that they consent.

### 10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

The OPC takes the position that zombie cookies, supercookies, third-party cookies that appear to be first-party cookies, device fingerprinting and other techniques that cannot be controlled by individuals are not permitted pursuant to PIPEDA as they do not permit individuals to effectively opt-out of the collection and use of their PI.

The OPC also takes the position that organisations should avoid knowingly tracking children, including by using cookies or other tracking technologies on websites aimed at children.

### 10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

Yes; there have been several regulatory investigations in relation to cookies.

For example, in PIPEDA Case Summary #2003-162, the OPC found that requiring users to consent to permanent cookies as a condition of accessing a website was a contravention of PIPEDA.

In PIPEDA Report of Findings #2013-003, the OPC reiterated that organisations must disclose to website visitors the use of cookies and the purposes for which the organisation collects PI.

### 10.4 What are the maximum penalties for breaches of applicable cookie restrictions?

As noted at questions 9.7 and 15.4, CASL, Alberta PIPA and the Quebec Act allow for the imposition of administrative penalties or fines, which could be levied in the event of non-compliance related to cookies.

## 11 Restrictions on International Data Transfers

### 11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

The Principal Legislation generally allows for the transfer of PI to other jurisdictions if the organisation uses contractual or other means to provide a comparable level of protection while the PI is being processed abroad. However, certain restrictions and requirements may apply.

Organisations must assess risks that could jeopardise the integrity, security and confidentiality of PI when it is transferred outside of Canada. For example, the OPC has taken the position that the PI of individuals who purchase cannabis should generally be stored on a server located in Canada because cannabis use is illegal in most other countries. Organisations subject to PIPEDA must also advise individuals that their PI may be sent to another jurisdiction for processing and may be accessed by foreign courts, law enforcement and national security authorities.

Under Alberta PIPA, an organisation who uses a service provider (including a parent corporation, subsidiary or affiliate) outside of Canada to collect, use, disclose or store PI must have policies and practices regarding: (i) the countries outside Canada in which the collection, use, disclosure or storage of PI is occurring or may occur; and (ii) the purposes for which the service provider outside Canada has been authorised to collect, use or disclose PI for or on behalf of the organisation. The organisation must, prior to or at the time of collecting or transferring the PI, notify the individual of the way in which they may obtain written information regarding the organisation's policies and practices with respect to service providers outside of Canada and the name or position/title of a person who is able to answer questions about the collection, use, disclosure or storage of PI by such service providers.

Pursuant to the Quebec Act, prior to communicating or entrusting PI to a person outside of Quebec with the task of holding, using or communicating such PI on the organisation's behalf, an organisation must first take all reasonable steps to ensure: (i) that the PI will not be used for irrelevant purposes or communicated to third parties without the individual's consent; and (ii) in the case of nominative lists, that individuals have a valid opportunity to refuse that their PI be used for purposes of commercial or philanthropic prospection and, if need be, to have such PI deleted from the list. If the organisation determines that this level of protection will not be afforded to the PI,

the organisation must refuse to communicate or entrust the PI to a party outside of Quebec.

Some public and health sector privacy statutes also include requirements and/or restrictions applicable to transferring PI outside of Canada or the relevant province.

**11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).**

Organisations typically enter into data processing agreements to ensure that PI transferred outside of Canada is provided a comparable level of protection. While the consent of the individual to such a transfer is not generally required under the Principal Legislation, organisations must satisfy all statutory requirements, including those described at question 11.1.

**11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.**

No, transfers of personal data to other jurisdictions do not require registration with, notification to or prior approval from the relevant data protection authority(ies).

**11.4 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?**

To date, Canadian privacy regulators have not released guidance with respect to the *Schrems II* decision. PIPEDA is currently considered "adequate" for the purposes of permitting transfers of personal data from the EU to Canada. In addition, the federal government and Quebec's provincial government have proposed significant reforms to PIPEDA and the Quebec Act, respectively, which, if passed, would align with several of the General Data Protection Regulation's ("GDPR") standards.

**11.5 What guidance (if any) has/have the data protection authority(ies) issued in relation to the European Commission's revised Standard Contractual Clauses?**

To date, Canadian privacy regulators have not released guidance with respect to the EU Commission's revised standard contractual clauses. See above regarding PIPEDA's adequacy designation.

## 12 Whistle-blower Hotlines

**12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?**

The Principal Legislation does not expressly prohibit or restrict the establishment of whistle-blower hotlines.

An OPC investigation into the use of a whistle-blower system by a government entity suggested that organisations considering using a whistle-blower hotline must balance the expectations of confidentiality and anonymity for reporters with procedural fairness concerns for individuals who are subject to an investigation.

Whistle-blowers within federal institutions are afforded protections by the Public Servants *Disclosure Protection Act*, SC 2005 c 46.

**12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?**

To date, Canadian privacy regulators have not issued guidance or investigation reports discouraging or prohibiting anonymous reporting. Accordingly, anonymous reporting is generally permitted.

## 13 CCTV

**13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?**

There are no requirements for registration, notification or prior approval of the use of CCTV cameras under the Principal Legislation.

However, joint guidance from the OPC, Alberta Regulator and B.C. Regulator provides that organisations must post signs alerting an individual to the presence of a camera before they enter the premises. Such signs should include a contact person in case individuals have questions or want access to their PI that is collected by the camera. Some Canadian privacy regulators have also recommended that the purpose(s) of the cameras should be disclosed.

**13.2 Are there limits on the purposes for which CCTV data may be used?**

PI collected through CCTV cameras may only be used for purposes that a reasonable person would consider appropriate in the circumstances. According to joint guidance from the OPC, Alberta Regulator and B.C. Regulator, examples of appropriate purposes may include security around banking machines or inside convenience stores in high-crime areas. Organisations should consider less privacy-invasive alternatives before installing CCTV cameras. The B.C. Regulator has also stated that video surveillance should be used only in response to a real and significant security or safety problem.

## 14 Employee Monitoring

**14.1 What types of employee monitoring are permitted (if any), and in what circumstances?**

Various types of employee monitoring have been upheld by Canadian privacy regulators and adjudicators in certain circumstances, including video surveillance, monitoring employees' use of information technology, recording telephone calls, and GPS tracking. However, such monitoring must be carried out in accordance with applicable privacy laws and may also have employment and labour law implications.

Canadian privacy regulators and adjudicators have developed different tests to evaluate when employee monitoring is acceptable. Common considerations in assessing whether employee monitoring is reasonable include: (i) whether there is a legitimate issue or demonstrable need to be addressed through the monitoring; (ii) whether the monitoring is likely to be effective in addressing that issue or meeting that need; (iii) whether the loss of privacy is proportional to the benefit gained through the monitoring; and (iv) whether there is a less privacy-invasive way of achieving the same end. In assessing whether the monitoring is reasonable, some privacy regulators and adjudicators have also considered the sensitivity of the PI collected, whether the monitoring is covert, and whether the employee had a subjective expectation of privacy.

**14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.**

PIPEDA, Alberta PIPA and B.C. PIPA permit employers to collect, use and disclose employees' PI without their consent, provided such collection, use and disclosure is only for purposes reasonably required to establish, manage or terminate an employment relationship. However, the employer must still provide the individual with advance notice that their PI will be collected, used or disclosed and the purposes for doing so, in addition to complying with all other statutory requirements.

In Quebec, employees' consent to the collection, use and disclosure of their PI through monitoring will generally be required, subject to limited exceptions.

Employers may also be subject to statutory and/or common law tort claims related to employee monitoring, including claims that unreasonable monitoring constitutes an intrusion upon seclusion.

In practice, most employers provide notice and/or obtain consent to collect PI through employee monitoring via employment agreements, policies that are brought to employees' attention (e.g., workplace privacy policies, acceptable use policies, etc.) and/or by using signage in the workplace.

**14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?**

Employers should consult the terms of any applicable collective agreements in order to determine whether a union or employee association must be notified of, or consulted with respect to, the implementation of employee monitoring.

Even where such an obligation does not exist by operation of a collective agreement, employers may strategically decide to advise a union or employee association of the implementation of employee monitoring in order to obtain feedback and potentially lower the risk of a policy grievance or other objection once the monitoring is implemented.

## 15 Data Security and Data Breach

**15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?**

The Principal Legislation generally requires that an organisation must protect PI against loss or theft, as well as unauthorised access, disclosure, copying, use or modification using physical, organisational and technological measures that are appropriate to the sensitivity of the PI as well as the amount, distribution, and format of the information, and the method of storage.

An organisation that transfers PI to a third party for processing must use contractual or other means to protect such PI, including by ensuring that a processor also implements appropriate safeguards.

Some industry regulators, including the CSA, OSFI, IIROC and MFDA (as defined at question 1.3), require organisations to monitor, detect, prevent and/or mitigate incidents involving PI and other cyber-incidents.

**15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

PIPEDA requires an organisation to report to the OPC a loss of, unauthorised access to or unauthorised disclosure of PI resulting from a breach of the organisation's security safeguards or from a failure to establish those safeguards (a "**Breach of Security Safeguards**") where it is reasonable in the circumstances to believe that the Breach of Security Safeguards creates a real risk of significant harm ("**RROSH**") to any individual(s) (a "**Reportable Breach**").

The report must be made as soon as feasible after the organisation determines that a Reportable Breach has occurred, and must be in writing and contain (to the extent known):

- a description of the circumstances of the Reportable Breach and the cause;
- the day on which, or the period during which, the Reportable Breach occurred;
- a description of the PI that is the subject of the Reportable Breach;
- the number of individuals affected by the Reportable Breach;
- a description of the steps that the organisation has taken to reduce the risk of harm to individuals that could result from the Reportable Breach, or to mitigate that harm;
- a description of the steps that the organisation has taken or intends to take to notify affected individuals of the Reportable Breach; and
- the name and contact information of a person who can answer the OPC's questions about the Reportable Breach.

PIPEDA also requires organisations to advise any organisation or governmental institution that may be able to reduce or mitigate the risk of harm arising from the Reportable Breach.

Alberta PIPA also requires that an organisation having PI under its control provide notice, without unreasonable delay, to the Alberta Regulator of any incident involving the loss of or unauthorised access to or disclosure of PI where a reasonable person would consider that there exists a RROSH to an individual as a result of the loss or unauthorised access or disclosure. The contents of the notice are prescribed by Section 19 of the *Personal Information Protection Act Regulation*, Alta Reg 366/2003.

The B.C. Regulator and the Quebec Commission also generally expect voluntary reporting of breaches that give rise to a RROSH.

Public sector legislation and health sector legislation in some provinces and territories also include breach reporting requirements.

Some industry regulators, including the CSA, OSFI, IIROC and MFDA (as defined at question 1.3), require organisations to report or disclose certain breaches/incidents to the regulators.

**15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

PIPEDA requires that organisations notify individuals of any Reportable Breach as soon as feasible. Such notice must contain sufficient information to enable individuals to understand the significance of the Reportable Breach to them and to take steps to reduce or mitigate the risk of harm, and must also contain certain prescribed content, including (without limitation) a description of the Reportable Breach, timing of the Reportable Breach, the PI impacted and the steps taken by the organisation to mitigate or reduce the risk of harm.

Under Alberta PIPA, the Alberta Regulator can require an organisation to notify individuals to whom there is a RROSH as a result of a breach. The contents of the notice (if required) are prescribed by Section 19.1(1) of the *Personal Information Protection Act Regulation*, Alta Reg 366/2003.

The B.C. Regulator and the Quebec Commission also generally expect voluntary notification of breaches that give rise to a RROSH, and failure to do so can increase litigation risk.

**15.4 What are the maximum penalties for data security breaches?**

The OPC can make non-binding recommendations in the event of non-compliance with PIPEDA, including a failure to implement adequate safeguards to protect PI from Breaches of Security Safeguards. Following the OPC's issuance of recommendations, an application can be made to the Federal Court for relief, including damages to complainants. The Attorney General can prosecute an organisation for failing to comply with the breach reporting, notification and recording obligations under PIPEDA, which can result in fines of up to $10,000 on summary conviction or $100,000 for an indictable offence.

Under Alberta PIPA, an organisation that collects, uses or discloses PI in contravention of Alberta PIPA, or that fails to comply with its breach reporting obligations, can be subject to fines up of to $10,000 for an individual or $100,000 for a person other than an individual.

Under the Quebec Act, an organisation that collects, holds, communicates to third parties or uses PI in contravention of the Quebec Act is liable to a fine of $1,000 to $10,000 for a first offence and $10,000 to $20,000 for a subsequent offence.

Individuals whose PI is compromised by a privacy or security breach can also bring civil tort claims for damages, either on an individual basis or as part of a class action proceeding.

## 16 Enforcement and Sanctions

**16.1 Describe the enforcement powers of the data protection authority(ies).**

(a) **Investigative Powers**: Canadian privacy regulators are generally empowered to conduct investigations into organisations' compliance with the Principal Legislation. The scope of the regulators' investigative powers is set out in the applicable legislation, and may include, for example, the ability to compel oral or written evidence under oath, enter certain premises, and obtain or compel the production of certain records. Some regulators are also empowered to order or initiate mediation, hearings and/or inquiries into complaints of non-compliance with privacy legislation and/or to enter into voluntary compliance agreements with organisations that have been found to have contravened privacy legislation.

(b) **Corrective Powers**: At the conclusion of an investigation under PIPEDA, the OPC will typically issue a report of findings, including the conclusions of its investigation and non-binding recommendations to rectify and prevent the reoccurrence of non-compliance. Following the OPC's report, an application can be made to the Federal Court, where a variety of remedial orders (including damages to complainants) can be issued. Both the Alberta Regulator and B.C. Regulator can issue binding orders against an organisation following an inquiry. If such an order is issued, both Alberta PIPA and B.C. PIPA provide that (an) affected individual(s) can bring an action against the organisation for damages for loss or injury caused by the organisation's actions. The Quebec Act provides that, following an inquiry, the Quebec Commission may recommend or order the application of such remedial measures as are appropriate to ensure the protection of PI.

(c) **Authorisation and Advisory Powers: Canadian privacy regulators may play a variety of advisory roles, for example by**: (i) providing independent reviews and resolutions of requests and complaints related to access to information requests and the handling of PI; (ii) advising and making recommendations about the application of privacy legislation to stakeholders; and (iii) commenting on the privacy implications of proposed legislation, programmes or policies or new technologies. The regulators also publish guidance documents (often jointly) regarding the interpretation and application of privacy and data protection laws.

(d) **Imposition of administrative fines for infringements of specified GDPR provisions**: Canadian privacy regulators are not empowered to impose administrative fines for non-compliance with the GDPR. However, as set out at questions 15.4 and 16.1(e), some regulators may be able to issue fines for infringements of the Principal Legislation.

(e) **Non-compliance with a data protection authority**: Under PIPEDA, if an organisation fails to abide by the terms of a voluntary compliance agreement with the OPC, the OPC may apply to the Federal Court for relief, including an order requiring the organisation to comply with the terms of the compliance agreement. In Alberta, an order of the Alberta Regulator can be filed with the Court of Queen's Bench and thereafter becomes enforceable as a judgment or order of that court. Failing to comply with an order of the Alberta Regulator is an offence and is subject to the maximum penalties set out at question 15.4. A person who fails to comply with an order of the B.C. Regulator is guilty of an offence and is liable, if an individual, to a fine of not more than $10,000, and, if a person other than an individual, to a fine of not more than $100,000. An order of the Quebec Commission can also be filed and executed as a judgment of Quebec's Superior Court.

**16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?**

As set out at question 16.1, Canadian privacy regulators generally have the ability to make recommendations or issue orders, including, in some cases, requiring an organisation to stop collecting, using or disclosing PI in contravention of the

Principal Legislation. Enforcing such a recommendation or order may require the regulator to either file the order with the court or, in the case of PIPEDA, apply to the Federal Court for relief.

**16.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.**

The OPC and provincial privacy regulators chiefly take a collaborative approach to resolving privacy complaints, which includes making recommendations and issuing joint reports. The OPC has also worked in coordination with privacy authorities from other countries to arrive at joint findings (see, for example, PIPEDA Report of Findings #2018-003).

On rare occasions, the OPC has entered into voluntary compliance agreements (see PIPEDA Report of Findings #2018-006 and #2016-005). The OPC last applied to the Federal Court for a *de novo* hearing in 2017 (see PIPEDA Report of Findings #2017-007).

Investigations of possible contraventions of Canadian privacy laws can be initiated by complaints from individuals (see PIPEDA Report of Findings #2020-001), following data breach disclosures by organisations (see PIPEDA Report of Findings #2020-005), or, increasingly, by the privacy regulators themselves working proactively (see PIPEDA Report of Findings #2020-004).

**16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?**

Yes; see question 3.1.

In *A.T. v. Globe 24h.com*, 2017 FC 114, the Federal Court found that PIPEDA had extraterritorial application to a website operated out of and hosted on a server in Romania because there was a "real and substantial link" between the website's activities and Canada. The fact that Romanian authorities had already acted to curtail the website's activities did not preclude PIPEDA from applying where the activities had unlawful consequences in Canada.

## 17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

**17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?**

Organisations should consult applicable privacy legislation to confirm whether such disclosure of PI is lawful and, if so, whether the individual's consent to such disclosure is required.

For example, PIPEDA provides that an organisation may disclose PI without the knowledge or consent of an individual if: (i) the disclosure is made to a government institution (or part of a government institution) that has made a request for the PI, identified its lawful authority to obtain the PI, and indicated that the disclosure is requested for the purpose of enforcing any law of a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law; or (ii) the disclosure is required to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records.

**17.2 What guidance has/have the data protection authority(ies) issued?**

In its *Guidelines for Processing Personal Data Across Borders*, the OPC advises that organisations that transfer PI outside of Canada for processing must make it plain to individuals that their PI may be processed in a foreign country and, therefore, may be accessible to law enforcement and national security authorities of that jurisdiction. Organisations must do this in clear and understandable language, typically at the time the PI is collected.

In *PIPEDA and Your Practice: A Privacy Handbook for Lawyers*, the OPC advises both lawyers and their clients to be particularly sensitive to the requirements of PIPEDA during e-discovery. The OPC notes that Canadian courts have repeatedly rejected requests for production of entire hard drives and other electronic information on the grounds that such production constitutes an unjustified invasion of privacy. Courts can also impose privacy-protective measures to ensure that the invasion of privacy is kept to a minimum. Lawyers and clients who hire service providers to assist in managing e-discovery issues must also satisfy themselves that those service providers will comply with PIPEDA, including by using contractual or other means to ensure that PI receives a comparable level of protection while being processed by the service provider and giving notice to individuals if their PI will be processed outside of Canada (however, the OPC recognises that the latter may not be feasible with respect to PI received from an opposing party during e-discovery).

## 18 Trends and Developments

**18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.**

In the past year, Canadian privacy regulators have combined their resources to conduct several joint investigations, including:

- an investigation by the OPC, the Alberta Regulator and the B.C. Regulator into the collection and use of PI (including biometric information) of visitors to malls via anonymous video analytics technology installed in wayfinding directories and mobile device geolocation tracking technologies (PIPEDA Report of Findings #2020-004);
- an investigation by the OPC and Quebec Commission into a data breach by an employee that ex-filtrated the PI of close to 9.7 million individuals in Canada and abroad over a period of 26 months (PIPEDA Report of Findings #2020-005); and
- an investigation into the facial recognition tool of Clearview AI, Inc. by the OPC, the Quebec Commission, the Alberta Regulator and the B.C. Regulator (PIPEDA Report of Findings #2021-001).

The OPC has also recently focused on several complaints related to foreign processing of consumers' PI (see, for example, PIPEDA Report of Findings #2020-001 and #2020-003).

**18.2 What "hot topics" are currently a focus for the data protection regulator?**

- **Statutory reform, including stronger enforcement mechanisms** – For several years, the OPC has been advocating for significant reforms to Canadian privacy laws, including enhanced enforcement powers and significant penalties for non-compliant organisations. In November 2020, the federal government tabled Bill C-11 which, if

passed, would allow for significant administrative penalties for organisations that contravene federal privacy legislation, as well as establish a tribunal to adjudicate appeals from OPC orders. The provincial governments of Quebec and B.C. are also considering changes to strengthen their privacy legislation.

- **Privacy implications of new technologies** – Recent cases indicate that regulators are focused on the privacy impact of new technologies, including (without limitation) automatic scanning tools and the use of artificial intelligence.
- **Transborder dataflows** – International data processing has been a "hot topic" for several years, and Canada's approach to this issue is far from finalised.
- **Health privacy** – With new advances in online healthcare, health privacy issues are likely to be an area of interest to Canadian privacy regulators.

## Acknowledgment

Lyndsay and Kristen are grateful to Robbie Grant for his research and assistance with this chapter.

**Lyndsay A. Wasser** is the Co-Chair of McMillan's Privacy & Data Protection Group and its Cybersecurity Group. She is a Certified Information Privacy Professional/Canada and regularly advises and assists clients on a broad range of privacy and cybersecurity issues, including advising on legal requirements related to data security, workplace privacy issues, handling personal health information and transferring PI across borders. She assists clients to develop privacy compliance programmes and data sharing agreements. She has assisted many clients with responding to privacy and data breaches involving various types of information (e.g., payment card information, patient data, employee personal information and sensitive identity information), including assisting with risk assessment, breach response strategy, notification obligations and communications with regulators. Lyndsay regularly writes and speaks on cybersecurity topics and is the co-author of *Privacy in the Workplace*, 4th ed. and the privacy chapter in the *Ultimate Corporate Counsel Guide*.

**McMillan LLP**
Brookfield Place, Suite 4400
181 Bay Street
Toronto, Ontario
Canada
M5J 2T3

Tel: +1 416 865 7083
Email: lyndsay.wasser@mcmillan.ca
URL: www.mcmillan.ca

**Kristen Pennington** is a Partner in McMillan's Privacy & Data Protection and Cybersecurity Groups. Kristen advises organisations about legal requirements related to privacy and data protection, including employee background checks, cross-border transfers of personal information and the privacy implications of corporate transactions. She assists clients with developing practical, up-to-date privacy compliance programmes and with drafting appropriate waivers, consent forms and data sharing terms with service providers, affiliates and other third parties. An experienced advocate, Kristen has appeared before the Ontario Superior Court and the Ontario Court of Appeal and at various mediations. Kristen regularly writes and speaks about emerging Canadian privacy topics, including the rise of privacy torts in Canada and the processing of employee and third-party personal information in connection with COVID-19.

**McMillan LLP**
Brookfield Place, Suite 4400
181 Bay Street
Toronto, Ontario
Canada
M5J 2T3

Tel: +1 416 865 7943
Email: kristen.pennington@mcmillan.ca
URL: www.mcmillan.ca

McMillan is a leading Canadian business law firm with recognised expertise and acknowledged leadership in major business sectors, which provides solutions-oriented legal advice through its offices in Calgary, Montréal, Ottawa, Toronto, Vancouver and Hong Kong. McMillan's privacy law experts have a thorough understanding of legal and regulatory obligations related to privacy, data protection and cybersecurity, and regularly assist organisations by: advising on compliance with applicable privacy and data protection, anti-spam, misleading advertising and other legislation; drafting data protection policies, protocols and training materials; negotiating agreements with third-party suppliers and service providers while analysing privacy and data protection implications; strategic handling of data breaches; assisting vendors and purchasers with assessing the privacy law implications of corporate transactions; and advising on and defending claims related to data protection, including defending class action litigation.

**www.mcmillan.ca**

# China


Susan Ning


Han Wu

King & Wood Mallesons

## 1 Relevant Legislation and Competent Authorities

### 1.1 What is the principal data protection legislation?

The principal personal data protection legislation in China is the *Cybersecurity Law of the People's Republic of China* (hereinafter, the "**CSL**"). It sets out general data protection requirements for network operators. China is also preparing specific personal information protection law and data security law. Please refer to question 18.1 for more information.

### 1.2 Is there any other general legislation that impacts data protection?

There are pieces of civil and criminal legislation that have an impact on data protection.

In particular, the *Civil Code*, which took effect on 1 January 2021, establishes the right to privacy and the principles of personal information protection. It provides a definition of personal information and sets out the legal basis for personal information processing, the obligations on the personal information processors, the rights of individuals to their personal information and so on. Most of the provisions of the *Civil Code* regarding the protection of personal information are restatements of requirements contained in the CSL, and national standards such as the *National Standard of the People's Republic of China for Information Security Technology – Personal Data Security Specification*.

The *Criminal Law* also sets forth offences relating to infringing personal data and privacy, e.g., the offence of infringing citizens' personal information in Article 253-(1), the offence of refusing to fulfil information network security responsibilities in Article 286-(1), and the offence of stealing, purchasing or illegally disclosing other people's credit card information in Article 177-(1). The *Interpretation of Several Issues Regarding Application of Law to Criminal Cases of Infringement of Citizen's Personal Information Handled by the Supreme People's Court and the Supreme People's Procuratorate* issued in 2017 provides further explanation regarding the offences relating to infringing personal data and privacy.

Article 2 of the *Tort Liability Law* sets the right to privacy as one of the civil rights of citizens, along with right to life, right to health, etc.

### 1.3 Is there any sector-specific legislation that impacts data protection?

There are many specific pieces of legislation in sectors of banking, insurance, medical, credit information, telecommunications and automobiles that impact data protection, such as the *Securities Law of the People's Republic of China*, the *Implementing Measures of the People's Bank of China for the Protection of Financial Consumers' Rights and Interests*, the *Measures for Administration of Population Health Information*, the *Medical Records Administration Measures of Medical Institutions*, the *Administrative Regulations on Credit Investigation Industry*, the *Several Provisions on Regulating the Market Order of Internet Information Services*, the *Measures for the Administration of Internet Email Services*, and the *Provisions on Protecting the Personal Information of Telecommunications and Internet Users*, etc.

### 1.4 What authority(ies) are responsible for data protection?

China has no single authority responsible for enforcing provisions relating to the protection of personal information.

Under the CSL, the Cyberspace Administration of China ("**CAC**") is responsible for the planning and coordination of cybersecurity and relevant supervisory and administrative work, while the Ministry of Industry and Information Technology ("**MIIT**"), the public security department and other relevant departments are responsible for the supervision and administration of personal information protection in their respective sectors.

For example, the Ministry of Public Security ("**MPS**") and its local branches are entitled to impose administrative penalties and are also in charge of criminal investigations against the unlawful obtaining, sale or disclosure of personal information.

The MIIT and the telecommunications administrations at the provincial level are responsible for the supervision and administration of personal information in the telecommunications and internet sector.

Also, the State Administration for Market Regulation ("**SAMR**") and its local counterparts are responsible for the supervision and administration of personal information of consumers, pursuant to the *Law on Protection of the Rights and Interests of Consumers*.

## 2 Definitions

### 2.1 Please provide the key definitions used in the relevant legislation:

- "**Personal Data**"
  "Personal Data", or personal information as in Article 76-(5) of the CSL, refers to various information that is recorded in electronic or any other form and used alone or in combination with other information to identify a natural person, including but not limited to the name, date of birth, ID number, personal biological identification

information, address and telephone number of the natural person. The *Civil Code* provides a similar definition of personal information.

- "**Processing**"
  The *Civil Code* provides the definition of "Processing". Article 1035 provides that processing of personal information includes the collection, storage, use, processing, transfer, provision and disclosure of personal information, etc.
  The CSL only provides definitions for a few key terms, and some of the definitions hereby listed are from the *National Standard of the People's Republic of China for Information Security Technology – Personal Data Security Specification* (hereinafter, "**Standard**"). The Standard is issued by the General Administration of Quality Supervision, Inspection and Quarantine, and the Standardization Administration. Although not compulsory, it is considered good practice to follow. The Standard was updated in March 2020 and took effect in October 2020.
- "**Controller**"
  The CSL does not define "Controller", but Section 3.4 of the Standard defines it as organisations or individuals that have the right to decide on the processing purposes, methods and other aspects of personal data.
- "**Processor**"
  Under the CSL and the Standard, there is no corresponding concept of "Processor". However, the Standard provides the obligations that data processors should comply with in the case of "entrusted processing" in Section 9.1.
  The *Civil Code* defines "Information Processor" as individuals or entities that process personal information, which may include both "Controller" and "Processor".
  The new draft legislation *Personal Information Protection Law* (as introduced in question 18.1) also uses "Personal Information Processor", which is defined as any organisation or individual that independently determines the purpose and method of processing and other personal information processing matters.
- "**Data Subject**"
  The CSL, the *Civil Code*, and the draft *Personal Information Protection Law* do not define "Data Subject". The Standard defines it as the person identified by the personal data in Section 3.3.
- "**Sensitive Personal Data**"
  The CSL does not define "Sensitive Personal Data". Section 3.2 of the Standard defines it as the personal data that, if divulged, illegally disclosed or abused, can harm personal or property safety, or can easily result in damage to reputation, physiological as well as psychological health, or cause the person to be discriminated against. For example, an ID number, personal biological identification information, a bank account, the record and content of correspondence, credit information and the personal data of children under 14 years old, etc.
  Article 29 of the draft *Personal Information Protection Law* similarly defines sensitive personal information as personal information that may lead to discrimination or serious harm to personal or property security once disclosed or illegally used. Sensitive personal information includes an individual's race, ethnicity, religious belief, personal biological characteristics, medical health, financial accounts and personal whereabouts.
- "**Data Breach**"
  The CSL, the *Civil Code*, the draft *Personal Information Protection Law*, and the Standard do not define "Data Breach".
  The National Contingency Plan for Cyber Security Incidents issued by the CAC defines "Cybersecurity Incidents", which refers to incidents that cause harm to the network and information systems or data therein and adversely affect society due to human factors, hardware or software defects or failures, natural disasters, etc. Cybersecurity incidents can be divided into hazardous programme incidents, network attack incidents, information destruction incidents, information content security incidents, equipment and facility failures, catastrophic incidents, and other incidents.
- The Standard also provides definitions for other key terms, which, among others, include "**Anonymisation**" and "**De-identification**":
  - **Anonymisation**, as defined in Section 3.14, means making the data subject unidentifiable or unable to be correlated through technical processing of personal data, and the processed information cannot be restored. Anonymised personal data is no longer considered to be personal data.
  - **De-identification**, as defined in Section 3.15, means making the data subject unidentifiable or unable to be correlated if not combined with other information through the technical processing of personal data.

  The draft *Personal Information Protection Law* provides a similar definition of the two terms.

## 3 Territorial Scope

**3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?**

Article 5 of the CSL grants the authorities the power to monitor, prevent and manage cybersecurity risks and threats from other jurisdictions. Pursuant to Article 50, if any information from other jurisdictions is found to be prohibited by law, the CAC and competent authorities may take measures to block the transmission of such information. Pursuant to Article 75, the law applies to an overseas institution, organisation or individual that engages in activity that also endangers Critical Information Infrastructure ("**CII**"). Further, companies operating under the offshore model but providing services to Chinese clients/users may also be subject to the personal data protection rules established by the CSL, especially those on the cross-border transfer of data. However, the law does not clearly specify how to realise the sanctions. As such, the extent to which these provisions will be enforced abroad against overseas companies remains unclear.

The draft *Personal Information Protection Law* provides similar rules to the EU General Data Protection Regulation ("**GDPR**") regarding its jurisdiction over businesses located outside of China. Article 3 provides that the law shall apply to the processing of personal information of natural persons who are in China under any of the following circumstances, where the processing happens outside of China:

1) where the purpose is to provide products or services to natural persons in China;
2) where the purpose is to analyse and evaluate the activities of natural persons in China; and
3) other circumstances provided by laws and administrative regulations.

## 4 Key Principles

**4.1 What are the key principles that apply to the processing of personal data?**

- **Transparency**
  Article 41 of the CSL stipulates that network operators

shall make public the rules for collecting and using personal data, and expressly notify the purpose, methods and scope of such collection and use.

Section 4e) of the Standard also sets out transparency as one of the basic principles, stating that the scope, purpose and rules of personal data processing should be publicly available and be clear, understandable and fair, and subject to external supervision.

The same principle has also been included in the draft *Personal Information Protection Law*. According to Article 7, the principles of openness and transparency shall be observed in the processing of personal information; the rules for the processing of personal information shall be publicly disclosed, and the purpose, manners and scope of processing shall be explicitly indicated.

- **Lawful basis for processing**

Article 41 of the CSL and Article 1035 of the *Civil Code* require the network operators to abide by the "lawful, justifiable and necessary" principles when collecting and using personal data.

Section 5.1 of the Standard further explains what "lawful" means – data controllers shall not deceive, inveigle or mislead the data subject into disclosing personal data, shall not conceal that the product or service it provides collects personal data, shall not obtain personal data from illegal channels and shall not collect information prohibited by law.

Among others, consent is the most common method for achieving lawfulness. Section 4c) of the Standard lists consent as a basic principle, which requires a personal data controller to obtain the data subjects' permission on the purpose, methods, scope and rules, etc. of processing the data.

It is to be noted that consent does not always equal lawfulness; Section 5.6 of the Standard further provides exceptions to the requirement of obtaining consent, where consent is not necessary prior to the collection and use of personal data. Nonetheless, be sure to bear in mind that the Standard is not an enforceable legal text, but a set of recommendations. Therefore, it is recommended to always obtain a data subject's consent where possible.

It is worth noting that the draft *Personal Information Protection Law* attempts to develop the legal basis for processing personal information. Except for obtaining consent, Article 13 provides some other legal grounds for processing of personal information, including:

1) the processing is necessary for the conclusion or performance of a contract to which the individual is a party;
2) the processing is necessary to fulfil statutory duties and statutory obligations;
3) the processing is necessary to respond to public health emergencies or protect natural persons' life, health and property safety;
4) personal information is processed within a reasonable scope to conduct news reporting, public opinion-based supervision, and other activities in the public interest;
5) processing within a reasonable scope of personal information that is publicly disclosed in accordance with this *Personal Information Protection Law*; or
6) under any other circumstance as provided by any law or administrative regulation.

- **Purpose limitation**

Article 41 of the CSL requires that network operators shall not collect any personal data that is not related to the services it provides. In Section 4b) of the Standard, there is also the "Clear Purpose Principle", where a data controller must have a clear and specific purpose for processing personal data.

It is also prohibited under Article 6 of the draft *Personal Information Protection Law* to conduct personal information processing unrelated to the processing purpose.

- **Data minimisation**

The CSL does not expressly provide requirements for data minimisation but only generally requires network operators to only collect personal data relevant and necessary for the provision of their services to data subjects.

Section 5.2 of the Standard sets out that, except when otherwise agreed with data subjects, data controllers shall only process the minimum type and amount of personal data necessary to fulfil the purpose the data subject has given consent to. After the purpose is fulfilled, the personal data should be deleted or anonymised promptly.

Furthermore, Article 6 of the draft *Personal Information Protection Law* provides that personal information processing shall be for a definite and reasonable purpose and shall be limited to the minimum scope for achieving the purpose of processing. The draft *Personal Information Protection Law* further provides in its second-reviewed version that the processing of personal information shall be conducted in a way that has the least impact on the interests of individuals.

- **Proportionality**

There is no explicit rule providing for a "proportionality principle" under the CSL or the Standard, but the data minimisation principle under the CSL and the Standard as well as the draft *Personal Information Protection Law* is similar in essence to the "proportionality principle", with both emphasising "processing of personal data only within a proper and necessary scope".

- **Retention**

Section 6.1 of the Standard provides that the storage period of personal information shall be the shortest time necessary to realise the purpose of authorised use of personal information, unless otherwise provided by laws and regulations or otherwise authorised or agreed by the personal information subject.

The draft *Personal Information Protection Law* provides in its Article 20 that unless otherwise stipulated in laws or administrative regulations, the retention period of personal information shall be the shortest time necessary for achieving the purpose.

- **Other key principles**

Article 42 of the CSL and Section 4f) of the Standard provide that a data controller should have the security capabilities that match the security risks it faces and take adequate measures to protect the confidentiality, integrity and availability of personal data. Furthermore, Article 8 of the draft *Personal Information Protection Law* stipulates that the quality of personal information should be guaranteed, so as to avoid adverse effects on personal rights and interests caused by processing inaccurate and incomplete personal information.

## 5 Individual Rights

### 5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**

Section 8.1 of the Standard provides that a data controller should provide a personal data subject with access to:

1) the data or the type of data about him or her held by the controller;
2) the source(s) and the purpose of such personal data; and
3) the identity or type of any third party who has obtained the above personal data.

The *Civil Code* and the draft *Personal Information Protection Law* allow a data subject to consult or copy his or her personal information from any information processor.

- **Right to rectification of errors**
  Article 43 of the CSL provides that each individual is entitled to require any network operator to make corrections if he or she has found errors in such information collected and stored by such operator. The Standard, the *Civil Code* and the draft *Personal Information Protection Law* provide similar rules.
- **Right to deletion/right to be forgotten**
  Under Article 43 of the CSL, each individual is entitled to require a network operator to delete his or her personal data if he or she finds that the collection or use of such information by such operator violates the laws, administrative regulations or the agreement by and between such operator and him or her. In addition to the provisions under the CSL, the draft *Personal Information Protection Law* further clarifies the scenarios where the personal information shall be deleted, including: (i) where the purpose of processing has been achieved or it is no longer necessary to process personal information for achieving such purpose; (ii) where the personal information processor stops providing products or services or the agreed storage period has expired; and (iii) where the individual withdraws his/her consent; or (iv) other circumstances specified in laws and administrative regulations.
  Apart from the above circumstances, Section 8.3 of the Standard further provides that if the data controller shares and transfers the personal data to a third party, or publicly discloses the personal data illegally or in breach of the agreement between the controller and the subject, and the subject demands that the data be deleted, the controller should stop such sharing, transferring and publicly disclosing, and notify the relevant parties to delete the relevant data. Section 8.5 provides that a data subject shall be provided channels to close his or her account and the relevant personal data shall be deleted/anonymised; data controllers shall not set unnecessary or unreasonable conditions when data subjects request to close an account. Further, Section 6.4 provides that if a personal information controller suspends operation in regard to its products or services, it shall delete or anonymise the personal information it holds.
- **Right to object to processing**
  Under the draft *Personal Information Protection Law*, a data subject has the right to restrict or refuse others to process his/her personal information.
  Under the Standard, a data subject's withdrawal of consent can be seen as a right to object to processing. It is to be noted that, pursuant to Section 7.7 of the Standard, a personal data subject will not be provided with a right to object but a right to appeal and a right to obtain manual review of the decisions when such decisions are made by information systems based on automated decisions (such as personal credit, loan limits or interview screening based on user profiling), which significantly influence the data subject's rights and interests.
- **Right to restrict processing**
  The CSL does not provide explicitly for the right to restrict processing. Under the draft *Personal Information Protection Law*, a data subject has the right to restrict or refuse others to process his/her personal information.
- **Right to data portability**
  The CSL does not provide explicitly for the right to data portability. Section 8.6 of the Standard recommends data controllers to provide methods for data subjects to obtain copies of their personal information. The right of data portability is of two kinds: (1) the data controller provides a copy of certain personal data to the data subject; and (2) the data controller directly sends the copy to the third party designated by the data subject where technically feasible.
  The personal data that can be portable are confined to four kinds: data subjects' basic personal data; personal identification information; personal health and physiology information; and personal education and occupational information.
- **Right to withdraw consent**
  Personal data subjects have complete freedom and control in respect of the handling of their personal data. Although it is not explicitly provided in the CSL, Section 8.4 of the Standard provides practical guidelines regarding the revocation and modification of consent, and specially mentions two different scenarios: (1) the withdrawal of consent for refusing to receive commercial advertisements; and (2) the withdrawal of consent for data sharing, transfer and public disclosure. The draft *Personal Information Protection Law* states that an individual shall have the right to withdraw his or her consent to personal information processing activities conducted on the basis of his or her consent, and requires processors of personal information to provide convenient ways for data subjects to withdraw their consent.
- **Right to object to marketing**
  Section 8.4 of the Standard stipulates that data subjects have the right not to receive commercial advertisements that are based on their personal data.
- **Right to complain to the relevant data protection authority(ies)**
  The right of individuals to complain to data protection authorities has been recognised in a number of pieces of legislations. For example, Section IX of the Decision of the Standing Committee of the National People's Congress on Strengthening Network Information Protection provides that any organisation or individual has the right to report to the relevant authorities regarding the illegal or criminal conduct of stealing or otherwise unlawfully acquiring, selling or providing to others a citizen's personal electronic information. Further, the CSL provides in Article 14 that one could report acts that endanger network security to the CAC, telecom, and public security authorities.
- *Other key rights – please specify*
  The draft *Personal Information Protection Law* added a provision in its second-reviewed draft on the protection of personal information-related rights of the deceased, i.e., the rights of the deceased shall be exercised by his/her close relatives.

## 6 Registration Formalities and Prior Approval

### 6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

There are such requirements regarding the cross-border transfer of data. As for operators of CII, if the personal information or important data generated or collected by CII operators within the territory of China needs to be transferred abroad for business purposes, a security assessment shall be conducted pursuant to the measures developed by the CAC together with

competent departments of the State Council. Under the draft *Personal Information Protection Law*, personal information processors that process the personal information reaching or exceeding the threshold specified by the CAC in terms of quantity shall conduct the security assessment organised by the CAC if it is necessary to transfer personal information abroad.

Besides, according to certain draft regulations, network operators shall conduct security assessments on transmitting data abroad. Both the Cross-border Transfer of Personal Information (Draft for Comment) issued in June 2019 and the *Personal Information Protection Law* (Draft for Public Consultation) issued in October 2020 stipulate that before the cross-border transfer of personal information, network operators shall apply to the local cyberspace administrations at the provincial level for security assessment for cross-border transfer of personal information.

Furthermore, Article 28 of the Administrative Measures on Data Security (Draft for Comment) provides that network operators shall assess the potential security risks prior to releasing, sharing or selling important data or transferring such data abroad, and shall report to the competent regulatory department for approval. If the competent regulatory department is unclear, network operators shall report to the cyberspace administrations at the provincial level for approval. Apart from the outbound transmission of important data, the newly issued *Data Security Law* requires the processor to regularly carry out risk assessment on its important data processing activities, and submit the risk assessment report to the relevant competent authority.

### 6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

The Cross-border Transfer of Personal Information (Draft for Comment) stipulates in Article 4 that network operators shall provide the following materials for security assessment for cross-border transfer of personal information, and shall be responsible for the authenticity and accuracy of the materials:

1) an application form;
2) contracts signed between network operators and recipients;
3) reports on analysis of the security risks for cross-border transfer of personal information and security measures; and
4) other materials required by the national cyberspace administration.

Specifically, the contract of cross-border data transfer shall at least specify:

1) the purposes of cross-border transfer of personal information and the types and storage periods of such information;
2) the subjects of personal information are the beneficiaries of the terms in the contracts that involve the rights and interests of the subjects of personal information;
3) when the legitimate rights and interests of the subjects of personal information are damaged, they may directly claim compensation from either network operators or recipients or from both parties, or entrust an agent on their behalf to do so, and network operators or recipients shall provide compensation, unless it is proved that they have no liability;
4) if changes of the legal environment in the recipients' countries make it difficult to perform contracts, contracts shall be terminated, or security assessment shall be reconducted; and
5) the termination of contracts shall not exempt network operators and recipients from their responsibilities and duties stipulated in the relevant terms of the contracts concerning the legitimate rights and interests of the subjects of personal information, unless the recipients have destroyed the personal information received or have anonymised the information.

As for the report of risk assessment of important data processing, the *Data Security Law* requires the processors to include the types and quantities of important data to be processed, the details of data processing activities, the data security risks faced and the corresponding measures.

### 6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

Article 3 of the Cross-border Transfer of Personal Information (Draft for Comment) specifies that provision of personal information to different recipients shall be subject to separate security assessments, and multiple or continuous provision of personal information to the same recipient does not need go through multiple assessments.

Moreover, Article 3 provides that a new security assessment shall be carried out every two years or in case of changes of the purpose of cross-border transfer of personal information or the type or overseas storage period of such information.

### 6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

Please see question 6.1 regarding who must notify the authority.

### 6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

Please see question 6.2 regarding the information to be included in the notification.

### 6.6 What are the sanctions for failure to register/notify where required?

The Cross-border Transfer of Personal Information (Draft for Comment) does not specify the sanctions for average network operators. Article 18 only provides that network operators that transfer personal information across borders in violation of the provisions shall be punished in accordance with relevant laws and regulations.

Article 66 of the CSL sets out the sanctions for CII operators' failure to seek approval from the authority. Specifically, it shall be warned and ordered to make rectifications, and shall be subjected to confiscation of illegal earnings and a fine ranging from RMB50,000 to RMB500,000, and may be subjected to suspension of a related business, winding up for rectification, shutdown of websites and revocation of business licences. The supervisor directly in charge and other directly liable persons shall be subject to a fine ranging from RMB10,000 to RMB100,000.

Article 37 of the Administrative Measures on Data Security (Draft for Comment) provides that for any network operator violating the provisions, the competent departments shall, in

accordance with relevant laws and administrative regulations and depending on the circumstances, take disciplinary actions such as disclosing misconduct publicly, confiscating illegal incomes, suspending relevant business operations, ceasing business operation for rectification, shutting down websites, or revoking the relevant business permits or business licences. If the violation constitutes a crime, criminal liability shall be investigated.

As for the failure of reporting risk assessment of important data processing, the *Data Security Law* provides that the relevant processors shall be subject to an order to make corrections and a warning. They may concurrently be imposed a fine of RMB50,000 to RMB500,000, and the person directly in charge and any other directly liable person may be fined RMB10,000 to RMB100,000. Furthermore, the processors who refuse to make corrections or cause serious consequences (such as a large amount of data leakage) shall be fined RMB500,000 to RMB2 million. Such processors may also be ordered to suspend relevant business, suspend business for rectification, have their relevant business licences revoked, and the person directly in charge and other directly liable person may be fined RMB50,000 to RMB500,000. There are also administrative penalties on violation of national core data management rules and rules on cross-border transfer of important data.

### 6.7 What is the fee per registration/notification (if applicable)?

Currently, it remains unclear. Normally, such notifications are free of charge.

### 6.8 How frequently must registrations/notifications be renewed (if applicable)?

Please refer to question 6.3. Furthermore, Article 9 of the Cross-border Transfer of Personal Information (Draft for Comment) provides that network operators shall, before 31 December of each year, report the situations of cross-border transfer of personal information and contract performance in the current year to the local cyberspace administrations at the provincial level.

As for important data processing, the *Data Security Law* does not explicitly provide the frequency to renew the report.

### 6.9 Is any prior approval required from the data protection regulator?

For CII operators, it is widely recognised that prior approval is required when transferring data abroad for business needs.

For transfer of personal information by network operators, Article 5 of the Cross-border Transfer of Personal Information (Draft for Comment) provides the procedures for the cyberspace administrations to conduct the security assessment. Article 2 specifies that if it is identified by the security assessment that the cross-border transfer of personal information may affect national security or damage public interest, or that it is difficult to effectively protect the security of personal information, cross-border transfer of such information shall not be permitted.

As to transfer of important data, the Administrative Measures on Data Security (Draft for Comment) expressly require network operators to obtain prior approval of competent regulatory authorities or cyberspace administrations.

As for important data processing, there is no requirement of prior approval in the *Data Security Law*.

### 6.10 Can the registration/notification be completed online?

It remains unclear whether the notification can be completed online.

### 6.11 Is there a publicly available list of completed registrations/notifications?

No, but there are public records of the operators that violate the Provisions on Protecting the Personal Information of Telecommunications and Internet Users (the "**Provisions**"). It is provided in Article 20 of the Provisions that the telecommunications authorities record the activities of telecommunications business operators and internet information service providers that have violated the Provisions into their social credit files and make public such information.

### 6.12 How long does a typical registration/notification process take?

Article 5 of the Cross-border Transfer of Personal Information (Draft for Comment) provides that security assessment shall be completed within 15 working days, and the time limit may be appropriately extended for those with complex situations. Detailed implementation measures or guidelines are expected to be formulated.

## 7 Appointment of a Data Protection Officer

### 7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

It is provided in Article 21 of the CSL that network operators should appoint network security officers to protect the security of the network. Further, it is provided in Article 34 that a CII operator shall also appoint a security management officer. The appointment of such officers is mandatory. Furthermore, Section 11.1 of the Standard specifies that the personal data controller shall appoint a Data Protection Officer and set up a Data Protection Department.

The draft *Personal Information Protection Law* requires a personal information processor that processes personal information reaching or exceeding the threshold specified by the national CAC in terms of quantity to appoint a person in charge of personal information protection to be responsible for conducting supervision of personal information processing activities as well as the protection measures taken. Furthermore, where the personal information processor is located outside China, it shall establish a special agency or designate a representative within China to be responsible for relevant matters of personal information protection, and submit the name and contact information of relevant agency or the representative to the department performing duties of personal information protection.

### 7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

Although the appointment of a Data Protection Officer is a good practice to follow, set by the Standard, there is no sanction for failing to do so under the CSL. Nonetheless, there are sanctions

for failure to appoint a network security officer and, in case of a CII operator, a security management officer, under Article 59 of the CSL.

Operators that fail to appoint a network security officer can expect warnings and orders for rectifications. A fine ranging from RMB10,000 to RMB100,000 may be imposed if the operator refuses to make rectifications, or in case of severe consequential damage. A fine ranging from RMB5,000 to RMB50,000 may be imposed on the person directly in charge.

CII operators that fail to appoint a security management officer can expect warnings and orders for rectifications. A fine ranging from RMB100,000 to RMB1 million may be imposed if the operator refuses to make rectifications or in case of severe consequential damage. A fine ranging from RMB10,000 to RMB100,000 may be imposed on the person directly in charge.

Under the draft *Personal Information Protection Law*, any illegal processing of personal information, or failure to adopt necessary security protection measures shall be subject to order of rectification and confiscation of illegal gains; if rectification is refused, a fine of not more than RMB1 million shall be imposed on the processor; and a fine of not less than RMB10,000 but not more than RMB100,000 shall be imposed on the directly liable person in charge and other directly liable persons. Where the circumstances are serious, except for the order of rectification and confiscation of illegal gains, a fine of not more than RMB50 million or not more than 5% of its turnover of the previous year shall be imposed. The processor may also be ordered to suspend relevant business or to suspend business for rectification; its business licence may further be revoked. Furthermore, a fine of not less than RMB100,000 but not more than RMB1 million shall be imposed on the directly liable person in charge and other directly liable persons.

### 7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

If a Data Protection Officer fails to perform his or her duty with due diligence, then he or she may be accused of administrative or even criminal liabilities in respect of his or her role as a Data Protection Officer.

### 7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

The law and relevant rules do not specify whether a business can appoint a single Data Protection Officer to cover multiple entities.

### 7.5 Please describe any specific qualifications for the Data Protection Officer required by law.

Section 11.1 of the Standard specifies that the Data Protection Officer shall be a person with relevant management experience and professional knowledge of personal information protection.

### 7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

Section 11.1 of the Standard provides that the Data Protection Officer's responsibilities include but are not limited to:

1) comprehensive and overall implementation of the organisation's personal data security and direct responsibility for the personal data security;
2) organising the formulation of a personal information protection work plan and supervising its implementation;
3) drafting, issuing, implementing and regularly updating the privacy policy and related regulations;
4) establishing, maintaining, and updating the list of personal data held by the organisation (including the type, amount, origin, recipient, etc. of the personal data) and authorised access policies;
5) conducting a personal data security impact assessment, proposing countermeasures and suggestions for personal information protection, and urging the rectification regarding security risks;
6) organising personal data security training;
7) conducting product or service testing before its release in case of unknown collection, use, sharing and other processing activities of personal data;
8) announcing information such as complaint or reporting methods and promptly accepting the complaint and report;
9) conducting safety audits; and
10) communicating with supervisory authorities, and reporting on personal information protection and incident handling, etc.

### 7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

The currently effective law does not require the appointment of a Data Protection Officer to be registered or notified to the relevant data protection authorities.

Under the draft *Personal Information Protection Law*, the name, contact information, among others, of the person in charge of personal information protection shall be submitted to the competent authority.

### 7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

Section 5.6 of the Standard provides the contents that the privacy policy should include, and the name of the Data Protection Officer is not within it. Nevertheless, it is recommended to appoint a person whom the public can contact for the purpose of dealing with users' queries and complaints regarding privacy and data protection issues.

Under the draft *Personal Information Protection Law*, a personal information processor shall publish the contact information of the person in charge of personal information protection.

## 8 Appointment of Processors

### 8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

The currently effective law does not have such requirements, but Article 9.1 of the Standard provides that a data controller may enter into an agreement with a trusted processor for it to process personal data on the controller's behalf. Furthermore, the draft *Personal Information Protection Law* requires a personal information processor who entrusts others to process personal information, to agree with the entrusted party on the purposes of the entrusted processing, processing period, processing methods, categories of personal information, protection measures, as well as the rights and obligations of both parties, among others.

**8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?**

There is no requirement for the formalities of the agreement. As for the content, Article 9.1 of the Standard stipulates that it should address the responsibilities and duties of the processor, including the requirements for processing the personal data, whether it can reassign a processor, the assistance it shall provide to the data controller, the responsibility to give feedback to the data controller and the responsibility in respect of terminating the agreement.

## 9 Marketing

**9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).**

Pursuant to Article 43 of the *Advertisement Law*, no organisation or individual shall, without obtaining the consent or request of the parties concerned, distribute advertisements to them via electronic means. Advertisements distributed via electronic means shall state the true identity and contact details of the senders, and the method for the recipients to refuse acceptance of future advertisements. Article 44 further provides that advertisements published in the form of pop-up windows on the website shall show the "close" sign prominently.

Article 13 of the Administration of Internet Electronic Mail Services Procedures provides that the word "advertisement" or "AD" must be indicated in the email subject, and it is prohibited to send emails containing commercial advertisement without the express consent of the receivers. Article 14 provides that if an email recipient who has expressly consented to receive electronic direct marketing subsequently refuses to continue receiving such emails, the sender shall stop sending such emails, unless otherwise agreed by the parties. The receivers shall be provided with the contact details for the discontinuation of the receipt of such emails, including the email address of the sender, and shall ensure that such contact details are valid within 30 days.

**9.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?**

The Advertisement Law as well as the Administration of Internet Electronic Mail Services Procedures do not specify whether they are only applicable to business-to-consumer marketing.

**9.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).**

Section VII of the Decision of the Standing Committee of the National People's Congress on Strengthening Network Information Protection provides that any organisation or individual shall not send commercial electronic messages to the fixed-line, mobile telephone or email inbox of an electronic message receiver without the prior consent or request of the receivers or if the receivers explicitly express rejection.

The operators of an e-commerce platform, when displaying search results of goods or services, shall mark "advertisement" for bid-ranked products or services, pursuant to Article 40 of the *E-commerce Law*. Furthermore, Article 18 provides that e-commerce business operators who provide search results based on consumers' preference or consumption habits shall in the meantime provide options not targeting consumers' personal characteristics.

As for marketing by means of automated decision making, the draft *Personal Information Protection Law* requires the relevant processor to provide options not specific to individuals' characteristics simultaneously, or provide methods for individuals to refuse such marketing or push.

**9.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?**

The CSL, the *Advertisement Law* and the *E-commerce Law* apply to operators providing products and services within the territory of the PRC, while for foreign operators providing products or services to the PRC on an offshore model, the law does not further elaborate whether it will apply or not. However, according to Article 3.2 of the Draft Security Assessment Guidelines on Cross-border Data Transfer, business operators not registered in China but providing products or services to China using the Chinese language, making settlement by the RMB, and delivering products to China are considered to be "providing products or services to China", in which case we understand that it is possible that the relevant provisions will apply. The draft *Personal Information Protection Law* applies to the processing of personal information of natural persons within China for the purpose of providing products or services to natural persons within China or analysing or assessing the conduct of natural persons in China. Therefore, the marketing sent by a personal information processor from other jurisdictions could be subject to the draft *Personal Information Protection Law* if it falls in the cases above.

**9.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?**

The Administration for Market Regulation is mainly responsible for the enforcement of marketing restrictions. There are recent cases where authorities such as the Administration for Market Regulation are taking action. For example, in 2017, Shanghai Paipaidai Financial Information Service Co., Ltd. was fined RMB800,000 for its infringement of the *Advertisement Law*, the breaches including, among others, sending direct advertisements via email without obtaining prior consent of the recipients.

**9.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?**

If the source of the marketing lists is legitimate and lawful and the data subject has consented, then it is not prohibited. Otherwise, it is illegal to do so, as network service providers and other enterprises, public institutions and their employees are obligated to keep strictly confidential a citizen's personal electronic information collected during their business activities, and may not disclose, falsify, damage, sell or illegally provide such information to others, as provided in the Decision of the

Standing Committee of the National People's Congress on Strengthening Network Information Protection.

**9.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?**

Article 63 of the Advertisement Law provides that sending direct marketing communications without obtaining the consent of the target may result in a fine of up to RMB30,000.

E-commerce platforms not clearly marked "advertisement" for bid-ranked products may face a fine of up to RMB100,000, pursuant to Article 81 of the *E-commerce Law* and Article 59 of the *Advertisement Law*.

In addition, Article 77 of the *E-commerce Law* provides that e-commerce business operators who provide search results in violation of Article 18 as described in question 9.2 shall be ordered to make the correction within a stipulated period, their illegal income shall be confiscated, and a fine ranging from RMB50,000 to RMB200,000 may be imposed. In serious cases, a fine ranging from RMB200,000 to RMB500,000 should be imposed concurrently.

As for the penalties under the draft *Personal Information Protection Law*, please refer to question 7.2.

## 10 Cookies

**10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).**

There is no legislation addressing the use of cookies explicitly. Given that cookies fall within the definition of personal information (the CSL stipulates that personal data refers to information that can be used alone or in combination with other information to identify a natural person, while the Standard also provides that information such as online browsing records is personal data), it is understood that the general regulations on personal data apply to the use of cookies.

**10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?**

The law does not distinguish between different types of cookies at this stage.

**10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?**

There are no administrative actions on the use of cookies. Nonetheless, in 2015, the search engine Baidu's use of cookies to personalise advertisements aimed at consumers when they enter certain third-party websites was found by the court not to infringe an individual's right to privacy.

**10.4 What are the maximum penalties for breaches of applicable cookie restrictions?**

Please refer to the maximum penalties for other general breaches.

## 11 Restrictions on International Data Transfers

**11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.**

The CSL provides that the personal information and important data collected by a CII operator during their operations within the territory of China shall be stored domestically, and the cross-border transfer of personal information and important data by a CII operator for business needs shall be subject to a security assessment.

For restrictions on international transfer of personal information and important data, please refer to questions 6.1–6.12. It is anticipated that both the Cross-border Transfer of Personal Information (Draft for Comment) and the Administrative Measures on Data Security (Draft for Comment), which are still under review by the relevant authorities, will be subject to further revision.

It remains uncertain whether the current requirements in the draft measures will take effect in the future.

**11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).**

With the data subjects' consent, companies can transfer data abroad provided a security assessment is properly carried out. In addition to obtaining the data subject's consent, companies would need to prove that their transfer of personal data overseas arose from business needs under certain circumstances, and shall submit security assessment results with competent authorities for approval according to the draft measures (see question 11.1).

The draft *Personal Information Protection Law* attempts to develop the rules on cross-border data transfer. Article 38 provides that where a personal information processor needs to provide personal information outside China due to business or other needs, it shall at least meet any of the following conditions:

1) security assessment organised by the national cyberspace administration has been passed;
2) personal information protection certification has been conducted by a specialised institution according to provisions issued by the national cyberspace administration;
3) a standard contract formulated by the CAC has been concluded with the overseas recipient, agreeing on both parties' rights and obligations, and supervision is conducted to ensure that personal information processing activities of the overseas recipient meet the personal information protection standards provided in this law; or
4) other conditions provided in laws or administrative regulations or by the CAC.

**11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.**

For CII operators, Article 37 of the CSL stipulates that personal

data and important data collected or generated in China must be stored domestically. The transfer of such information overseas arising out of business needs is permitted, subject to the prior consent of the data subject, completion of a security assessment and approval from competent industry authorities.

For general network operators' cross-border transfer of personal information and important data, please refer to questions 6.1–6.12.

**11.4 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?**

This is not applicable.

**11.5 What guidance (if any) has/have the data protection authority(ies) issued in relation to the European Commission's revised Standard Contractual Clauses?**

This is not applicable.

## 12 Whistle-blower Hotlines

**12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?**

The draft *Personal Information Protection Law* provides that any organisations and individuals shall have the right to file complaints or reports about illegal personal information processing activities with relevant authorities. The authorities receiving complaints or reports shall handle them without delay and notify the complainants and informants of the handling results.

**12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?**

The draft *Personal Information Protection Law* does not explicitly prohibit anonymous reporting. Anonymous reporting is generally permitted.

## 13 CCTV

**13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?**

Article 12 of the Public Security Video Image Information System Administrative Regulations (exposure draft, hereinafter the "**CCTV Regulations**"), which was issued by the MPS and regulates the use of CCTV for public safety purposes, stipulates that anyone who uses CCTV for public safety purposes shall notify the local public security department of the type and location of the camera installed.

**13.2 Are there limits on the purposes for which CCTV data may be used?**

Pursuant to Article 6 of the CCTV Regulations, it is prohibited to obtain state secrets, work secrets or trade secrets from a public security video image information system, or infringe on citizens' privacy by using such a system. Organisations that construct and use CCTV are required to keep in confidence the basic information (e.g., the system design, equipment type, installation location, address code) and collected data concerning state secrets, work secrets and trade secrets and shall not illegally disclose CCTV data concerning citizens' privacy. Such CCTV data shall not be bought or sold, illegally used, copied or disseminated, pursuant to Article 22.

According to Article 21, investigative, procuratorial and judicial powers, public security and national security organs, as well as the administrative departments of the government at or above town level, may inspect, copy or retrieve the basic information or data collected through CCTV.

Under circumstances of the security services, Article 25 of the Regulations on Administration of Security Services provides that the using of CCTV equipment shall not infringe on the legitimate rights and interests or privacy of individuals.

In the draft *Personal Information Protection Law*, the installation of image collection or personal identification equipment in public places shall be necessary for maintaining public security and comply with relevant regulations, and conspicuous signs shall be erected. The collected personal images and personal identification information can only be used for the purpose of maintaining public security, and shall not be disclosed to the public or provided to others, except with the separate consent of individuals.

## 14 Employee Monitoring

**14.1 What types of employee monitoring are permitted (if any), and in what circumstances?**

On the one hand, Article 8 of the *Labour Contract Law* provides that employers are entitled to know about basic information of the worker in direct relation to the labour contract between them; therefore, some types of employee monitoring are permitted, though no specific rule explicitly addresses employee monitoring. On the other hand, it is prudent that the monitoring shall not infringe the employee's privacy.

**14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.**

Yes, the collecting of personal data generally requires consent from the data subject – this principle also applies to employee monitoring. In practice, such consent is normally obtained through a provision in the labour contract or in the employee handbook or similar documents.

**14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?**

Article 4 of the *Labour Contract Law* requires employers to discuss

with the employee representatives' congress or all employees, and negotiate with trade unions or employee representatives when formulating, revising or deciding on matters directly involving the vital interests of workers such as remuneration, working hours, rest periods and days off, labour safety and health, insurance and welfare, staff training, labour discipline and labour quota administration, etc. Article 43 further provides that employers shall notify the trade union when they unilaterally rescind a labour contract. However, such notifying or negotiating circumstances may not directly relate to employers' monitoring or processing of employees' personal data.

## 15 Data Security and Data Breach

**15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?**

Under Article 40 of the CSL, network operators are responsible for taking technical and other necessary measures to ensure the security of personal data they collect, and to establish and improve the system for user information protection. However, if the network operator as a controller appoints a third party to process personal data on its behalf, it shall ensure that such processor will provide an adequate level of protection to the personal data involved, as provided in Section 8.1 of the Standard.

The draft *Personal Information Protection Law* similarly requires the processor of personal information to take necessary measures to ensure that personal information processing activities comply with the provisions of laws and administrative regulations, and prevent unauthorised access to as well as the leakage, theft, tampering or deletion of personal information. For the definition of personal information processor in the draft *Personal Information Protection Law*, please refer to question 2.1.

**15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

Yes. Under Article 42 of the CSL, in case of (possible) disclosure, damage or loss of data collected, the network operator is required to take immediate remedies and report to the competent authority. Section 9.1 of the Standard provides that the report should include the type, quantity, content and nature of the affected data subjects, the impact of the breach, measures taken or to be taken, and the contact information of relevant persons.

**15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

Yes. A network operator is required to take immediate remedies and notify the affected data subjects in case of (possible) data breaches pursuant to Article 42 of the CSL. Section 9.2 of the Standard stipulates that the content of the notification should include, but not be limited to, the nature and impact of the breach, the measures taken or to be taken, the suggestions for data subjects to mitigate risks, remedies for the data subjects and the contact information of the Data Protection Officer. Under the draft *Personal Information Protection Law*, notification to individuals may not be needed where the personal information processor is able to effectively avoid the harm caused by information leakage. However, if the relevant authority considers that the leakage may cause harm to individuals, it is entitled to require the personal information processor to notify individuals.

**15.4 What are the maximum penalties for data security breaches?**

Under Article 64 of the CSL, in case of severe violation, an operator or provider in breach of data security may face fines of up to RMB1 million (or 10 times the illegal earnings), suspension of a related business, winding up for rectification, shutdown of any website(s) and revocation of a business licence. The persons directly in charge may face a fine of up to RMB100,000. As for the penalties under the draft *Personal Information Protection Law*, please refer to question 7.2.

## 16 Enforcement and Sanctions

**16.1 Describe the enforcement powers of the data protection authority(ies).**

| Investigatory/ Enforcement Power | Civil/ Administrative Sanction | Criminal Sanction |
|---|---|---|
| The public security departments have investigatory power regarding criminal and administrative infringement on personal data, and enforcement power with relevant administrative and criminal sanctions. | The court is responsible for civil sanctions. | The court has the power to impose criminal sanctions. |
| The CAC, the telecommunications department, the public security department and other authorities concerned have investigatory power regarding administrative infringement on personal data, and enforcement power with relevant administrative sanctions. | The CAC, the telecommunications department, the public security department and other authorities concerned have the power to impose administrative sanctions. | This is not applicable. |

**16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?**

Yes, and no court order is needed. For example, pursuant to Article 50 of the CSL, if any information prohibited by laws and administrative regulations from release or transmission is found, the CAC and other competent authorities may require the

network operator to stop the transmission of such information, take measures such as deletion and keep the records. If any such information is from overseas, they may block the transmission.

**16.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.**

The CAC and relevant data protection authorities may issue a ban in the form of an administrative penalty, together with other punitive measures such as a fine, an order to rectify, etc. For relevant cases, please refer to question 18.2.

**16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?**

So far, there is no public record of Chinese data protection authorities exercising their powers directly against companies established in other jurisdictions. In most cases, authorities may talk with the local subsidiary of an international company for its violations of the CSL or other data protection regulations.

## 17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

**17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?**

In the case of foreign e-discovery requests from foreign law enforcement agencies, companies must obtain the consent of the personal data subject and carry out security assessments with the relevant authority before transmitting any personal data or important data abroad. In terms of security assessments of CIIs, the CSL provides that if there are different provisions under laws and administrative regulations, such provisions shall apply.

If there are treaties or agreements in relation to judicial assistance or cooperation entered into between China and the respective foreign country, the relevant companies may respond to such requests following such treaties or agreements. Furthermore, the *International Criminal Judicial Assistance Law* issued on 26 October 2018 sets out rules and procedures regarding the enforcement of international criminal judicial assistance in China, including assistance requests of domestic agencies to foreign authorities, and foreign agencies' requests of assistance in China. Pursuant to Article 4 of the *International Criminal Judicial Assistance Law*, domestic businesses must obtain authorisation from a competent authority of China before disclosing any information or providing any assistance requested by foreign law enforcement agencies.

Similar rules have been set in recent pieces of draft legislation. For example, pursuant to the draft *Personal Information Protection Law*, where it is necessary to provide personal information to any party outside of China for international judicial assistance or administrative law enforcement assistance, an application shall be filed with the relevant competent department for approval according to the law. Furthermore, the *Data Security Law* provides that the relevant Chinese authorities shall handle data requests of foreign judicial or administrative agencies in accordance with relevant laws and international treaties and agreements or in accordance with the principle of equality and reciprocity. Unless approved by relevant authorities, no domestic entity or individual is allowed to provide data stored in China to any foreign judicial or administrative agencies. Any entity or responsible person in violation of such requirement will be subject to administrative penalties.

**17.2 What guidance has/have the data protection authority(ies) issued?**

The CAC has not issued any guidance particularly concerning e-discovery requests from foreign law enforcement agencies.

## 18 Trends and Developments

**18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.**

2020 has seen an acceleration of developments in China's cybersecurity and data protection regimes. Most noticeable is the publication of two major pieces of legislations for public consultation.

On 21 October 2020, the Draft *Personal Information Protection Law* was finally unveiled to the public. By comprehensively deepening China's personal information protection system, the Draft strengthens the protection of personal information while taking into account the complexity of economic and social life. The release of the nearly 8,000-character Draft marks China's first attempt to systematically and legislatively define, establish, and integrate the provisions on the protection and regulation of personal information. The Draft not only incorporates China's legislative, regulatory and practical achievements regarding data security in recent years, including the CSL, but also takes references of the varied legislative experience of the other jurisdictions in data protection such as the GDPR. The Draft was further reviewed by the Standing Committee of the National People's Congress in 2021 and the second-reviewed version was released on 29 April 2021.

Furthermore, the Standing Committee of the National People's Congress published the Data Security Law on 10 June 2021, which will take effect on 1 September 2021. The *Data Security Law* stipulates that different security requirements will apply to data falling into different levels of sensitivity and relevant authorities will also formulate catalogues of "important data" within their jurisdictions, and implement enhanced security measures to protect these important data. It also stipulates that data activities that may affect national security will be subject to security reviews organised by government authorities.

**18.2 What "hot topics" are currently a focus for the data protection regulator?**

The illegal processing of personal information by apps and the ecological governance of network information are points of concern for data protection regulators at present.

During the year 2020, both the MPS and the MIIT have initiated a number of investigations on the illegal collection and use of personal information by app operators. As a result, lots of apps were notified by the authorities to make rectifications. In March 2021, the CAC, MPS, MIIT and SAMR issued the *Rules on the Scope of Necessary Personal Information for Common Types of Mobile Internet Applications*, which will take effect on 1 May 2021 and specify the scope of necessary personal information for 39 types of apps.

In January 2020, the CAC launched a six-month campaign of ecological governance of network information in order to rectify negative and harmful information such as obscene pornography, vulgarity, violence, terror, gambling scams, etc., on websites,

mobiles, forums, instant messaging tools, live broadcast platforms and other key links, and to investigate and close illegal websites and accounts.

In April 2020, the MPS launched the "Jingwang 2020" campaign to continue the fight against infringement of Chinese citizens' personal information.

In December 2020, the SAMR published its consultation draft of the *Antitrust Guidelines on the Platform Economy* where it points out that data may constitute necessary facilities under certain circumstances and data-driven algorithms may be used to reach monopoly agreements.

**Susan Ning** is a senior partner and the head of the Commercial and Regulatory Group. She is one of the pioneers engaged in the cybersecurity and data compliance practice, with publications in a number of journals such as the *Journal of Cyber Affairs*. Her publications include: *New Trends of the US Personal Data Protection – Key Points of the New FCC Rules*; *Big Data: Success Comes Down to Solid Compliance, Does Your Data Need a "VISA" to Travel Abroad?*; and *A Brief Analysis on the Impact of Data on Competition in the Big Data Era*, among others. Susan is recognised as a "Tier 1 Lawyer" for Cybersecurity and Data Compliance in *2019 LEGALBAND* China.

Susan's practice areas cover self-assessment of network security, responding to network security checks initiated by authorities, data compliance training, due diligence of data transactions or exchanges, compliance of cross-border data transmissions, etc. Susan has assisted companies in sectors such as IT, transportation, online payment, consumer goods, finance, internet of vehicles in dealing with network security and data compliance issues.

**King & Wood Mallesons**
18th Floor, East Tower
World Financial Center
1 Dongsanhuan Zhonglu, Chaoyang District
Beijing 100020
P. R. China

Tel: +86 10 5878 5010
Email: susan.ning@cn.kwm.com
URL: www.kwm.com

**Han Wu** practises in the areas of cybersecurity, data compliance and antitrust. He excels in providing cybersecurity and data compliance advice to multinational companies' branches in China from the perspective of data compliance in China. Han also has expertise in establishing network security and data compliance systems for Chinese enterprises going abroad in line with the requirements of the European Union (GDPR), the United States and other cross-jurisdictions. Han was elected as one of the "40-under-40 Data Lawyers" by *Global Data Review* in 2018, and was recognised as Next Generation Partner by *The Legal 500* in 2021.

In the area of cybersecurity and data compliance, Han provides legal services including: assisting clients to establish a cybersecurity compliance system; assisting clients in self-investigation on cybersecurity and data protection; assisting clients to conduct internal training on cybersecurity and data compliance; assisting clients in due diligence in data transactions; assisting clients to design plans for cross-border data transfers; and assisting clients in network security investigations and cybersecurity incidents, among others.

**King & Wood Mallesons**
18th Floor, East Tower
World Financial Center
1 Dongsanhuan Zhonglu, Chaoyang District
Beijing 100020
P. R. China

Tel: +86 10 5878 5749
Email: wuhan@cn.kwm.com
URL: www.kwm.com

# Cyprus


Loizos Papacharalambous

Anastasios Kareklas

Koushos Korfiotis Papacharalambous LLC


## 1 Relevant Legislation and Competent Authorities

### 1.1 What is the principal data protection legislation?

Since 25 May 2018, the principal data protection legislation in the EU has been Regulation (EU) 2016/679 (the "**General Data Protection Regulation**" or "**GDPR**"). The GDPR repealed Directive 95/46/EC (the "**Data Protection Directive**") and has led to increased (though not total) harmonisation of data protection law across the EU Member States. In Cyprus, a national law supplementing the GDPR was enacted in July 2018 (L.125(I)/2018).

### 1.2 Is there any other general legislation that impacts data protection?

The general legislation that impacts data protection in Cyprus is as follows:

- The Regulation of Electronic Communications and Postal Services Law of 2004, N.112(I)/2004 as amended to date, which implements the requirements of Directive 2002/58/EC (as amended by Directive 2009/136/EC) (the "ePrivacy Directive"), provides a specific set of privacy rules to harmonise the processing of personal data by the telecoms sector. In January 2017, the European Commission published a proposal for an ePrivacy Regulation (the "ePrivacy Regulation") that would harmonise the applicable rules across the EU. In September 2018, the Council of the European Union published proposed revisions to the draft. The ePrivacy Regulation is still a draft at this stage and it is unclear when it will be finalised.
- Law N.28(III)/2001 implementing the Convention for the Protection of Individuals with regard to automatic processing of Personal Data and Law N.30(III)/2003 implementing the Additional Protocol to the said Convention.
- The Access to Public Sector Information Law N.184(I)/2017 which was adopted and entered into force on 12 December 2020. This law provides citizens with the right to request and receive information, under certain conditions, from public authorities, and creates an obligation for public authorities to publish certain information on their websites to avoid submitting a request form to access this information. The Commissioner for Personal Data Protection was appointed as the supervisory authority for this law and will act as Information Commissioner. Article 3 (2) provides that the right to request access to information from public authorities does not apply if the request for information concerns personal data in which case the provisions of the GDPR and L.125(I)2018 will apply.

### 1.3 Is there any sector-specific legislation that impacts data protection?

The Prevention and Suppression of Money Laundering Activities Law (N.188(I)/2007), for example, imposes on the Compliance Officers of credit institutions the obligation to prepare and update lists categorising low- and high-risk clients with reference to their names, account numbers, etc.

### 1.4 What authority(ies) are responsible for data protection?

The Office of the Commissioner for Personal Data Protection ("the **Commissioner**") is the authority responsible for data protection.

## 2 Definitions

### 2.1 Please provide the key definitions used in the relevant legislation:

- "**Personal Data**" means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- "**Processing**" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- "**Controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- "**Processor**" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

- "**Data Subject**" means an individual who is the subject of the relevant personal data.
- "**Sensitive Personal Data**" are personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health or sex life and sexual orientation, genetic data or biometric data.
- "**Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

## 3 Territorial Scope

### 3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The GDPR applies to businesses that are established in any EU Member State, and that process personal data (either as a controller or processor, and regardless of whether or not the processing takes place in the EU) in the context of that establishment.

A business that is not established in any Member State, but is subject to the laws of a Member State by virtue of public international law, is also subject to the GDPR.

The GDPR applies to businesses outside the EU if they (either as controller or processor) process the personal data of EU residents in relation to: (i) the offering of goods or services (whether or not in return for payment) to EU residents; or (ii) the monitoring of the behaviour of EU residents (to the extent that such behaviour takes place in the EU).

Further, the GDPR applies to businesses established outside the EU if they monitor the behaviour of EU residents (to the extent such behaviour takes place in the EU).

## 4 Key Principles

### 4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  Personal data must be processed lawfully, fairly and in a transparent manner. Controllers must provide certain minimum information to data subjects regarding the collection and further processing of their personal data. Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
- **Lawful basis for processing**
  Processing of personal data is lawful only if, and to the extent that, it is permitted under EU data protection law. The GDPR provides an exhaustive list of legal bases on which personal data may be processed, of which the following are the most relevant for businesses: (i) prior, freely given, specific, informed and unambiguous consent of the data subject; (ii) contractual necessity (i.e., the processing is necessary for the performance of a contract to which the data subject is a party, or for the purposes of pre-contractual measures taken at the data subject's request); (iii) compliance with legal obligations (i.e., the controller has a legal obligation, under the laws of the EU or an EU Member State, to perform the relevant processing); or (iv) legitimate interests (i.e., the processing is necessary for the purposes of legitimate interests pursued by the controller, except where the controller's interests are overridden by the interests, fundamental rights or freedoms of the affected data subjects).
  Please note that businesses require stronger grounds to process sensitive personal data. The processing of sensitive personal data is only permitted under certain conditions, of which the most relevant for businesses are: (i) explicit consent of the affected data subject; (ii) the processing is necessary in the context of employment law; or (iii) the processing is necessary for the establishment, exercise or defence of legal claims.
- **Purpose limitation**
  Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes. If a controller wishes to use the relevant personal data in a manner that is incompatible with the purposes for which they were initially collected, it must: (i) inform the data subject of such new processing; and (ii) be able to rely on a lawful basis as set out above.
- **Data minimisation**
  Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed. A business should only process the personal data that it actually needs to process in order to achieve its processing purposes.
- **Accuracy**
  Personal data must be accurate and, where necessary, kept up to date. A business must take every reasonable step to ensure that personal data that are inaccurate are either erased or rectified without delay.
- **Retention**
  Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- **Data security**
  Personal data must be processed in a manner that ensures appropriate security of those data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- **Accountability**
  The controller is responsible for, and must be able to demonstrate, compliance with the data protection principles set out above.

## 5 Individual Rights

### 5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**
  A data subject has the right to obtain from a controller the following information in respect of the data subject's personal data: (i) confirmation of whether, and where, the controller is processing the data subject's personal data; (ii) information about the purposes of the processing; (iii) information about the categories of data being processed; (iv) information about the categories of recipients with whom the data may be shared; (v) information about the period for which the data will be stored (or the criteria used to determine that period); (vi) information about the existence of the rights to erasure, to rectification, to restriction of processing and to object to processing; (vii)

information about the existence of the right to complain to the relevant data protection authority; (viii) where the data were not collected from the data subject, information as to the source of the data; and (ix) information about the existence of, and an explanation of the logic involved in, any automated processing that has a significant effect on the data subject.
Additionally, the data subject may request a copy of the personal data being processed.

- **Right to rectification of errors**
  Controllers must ensure that inaccurate or incomplete data are erased or rectified. Data subjects have the right to rectification of inaccurate personal data.
- **Right to deletion/right to be forgotten**
  Data subjects have the right to erasure of their personal data (the "right to be forgotten") if: (i) the data are no longer needed for their original purpose (and no new lawful purpose exists); (ii) the lawful basis for the processing is the data subject's consent, the data subject withdraws that consent, and no other lawful ground exists; (iii) the data subject exercises the right to object, and the controller has no overriding grounds for continuing the processing; (iv) the data have been processed unlawfully; or (v) erasure is necessary for compliance with EU law or national data protection law.
- **Right to object to processing**
  Data subjects have the right to object, on grounds relating to their particular situation, to the processing of personal data where the basis for that processing is either public interest or legitimate interest of the controller. The controller must cease such processing unless it demonstrates compelling legitimate grounds for the processing which overrides the interests, rights and freedoms of the relevant data subject or requires the data in order to establish, exercise or defend legal rights.
- **Right to restrict processing**
  Data subjects have the right to restrict the processing of personal data, which means that the data may only be held by the controller, and may only be used for limited purposes if: (i) the accuracy of the data is contested (and only for as long as it takes to verify that accuracy); (ii) the processing is unlawful and the data subject requests restriction (as opposed to exercising the right to erasure); (iii) the controller no longer needs the data for their original purpose, but the data are still required by the controller to establish, exercise or defend legal rights; or (iv) verification of overriding grounds is pending, in the context of an erasure request.
- **Right to data portability**
  Data subjects have a right to receive a copy of their personal data in a commonly used machine-readable format, and transfer their personal data from one controller to another or have the data transmitted directly between controllers.
- **Right to withdraw consent**
  A data subject has the right to withdraw their consent at any time. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject must be informed of the right to withdraw consent. It must be as easy to withdraw consent as to give it.
- **Right to object to marketing**
  Data subjects have the right to object to the processing of personal data for the purpose of direct marketing, including profiling.
- **Right to complain to the relevant data protection authority(ies)**
  Data subjects have the right to lodge complaints concerning the processing of their personal data with the Commissioner's Office if the data subjects live in Cyprus or the alleged infringement occurred in Cyprus.
- **Right to basic information**
  Data subjects have the right to be provided with information on the identity of the controller, the reasons for processing their personal data and other relevant information necessary to ensure the fair and transparent processing of personal data.

## 6 Registration Formalities and Prior Approval

**6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?**

This is not applicable. Prior consultation is necessary in special circumstances: see question 11.3.

**6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?**

See question 6.1.

**6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?**

See question 6.1.

**6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?**

See question 6.1.

**6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?**

See question 6.1.

**6.6 What are the sanctions for failure to register/notify where required?**

See questions 6.1 and 15.1.

**6.7 What is the fee per registration/notification (if applicable)?**

See question 6.1.

**6.8 How frequently must registrations/notifications be renewed (if applicable)?**

See question 6.1.

**6.9 Is any prior approval required from the data protection regulator?**

See question 6.1.

**6.10 Can the registration/notification be completed online?**

See question 6.1.

**6.11 Is there a publicly available list of completed registrations/notifications?**

See question 6.1.

**6.12 How long does a typical registration/notification process take?**

See question 6.1.

## 7 Appointment of a Data Protection Officer

**7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.**

The appointment of a Data Protection Officer for controllers or processors is only mandatory in some circumstances, including where there is: (i) large-scale regular and systematic monitoring of individuals; or (ii) large-scale processing of sensitive personal data.

Where a business designates a Data Protection Officer voluntarily, the requirements of the GDPR apply as though the appointment were mandatory.

The Commissioner may establish and make public a list of processing operations and cases requiring the designation of a DPO, in addition to the cases referred to in Article 37 (1) of the GDPR.

**7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?**

In the circumstances where appointment of a Data Protection Officer is mandatory, failure to comply may result in the wide range of penalties available under the GDPR, including but not limited to Article 83 (4) (a) of the GDPR.

**7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?**

The appointed Data Protection Officer should not be dismissed or penalised for performing their tasks and should report directly to the highest management level of the controller or processor.

**7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?**

A single Data Protection Officer is permitted by a group of undertakings provided that the Data Protection Officer is easily accessible from each establishment.

**7.5 Please describe any specific qualifications for the Data Protection Officer required by law.**

The Data Protection Officer should be appointed on the basis of professional qualities and should have an expert knowledge of data protection law and practices. While this is not strictly defined, it is clear that the level of expertise required will depend on the circumstances. For example, the involvement of large volumes of sensitive personal data will require a higher level of knowledge.

**7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?**

A Data Protection Officer should be involved in all issues which relate to the protection of personal data. The GDPR outlines the minimum tasks required by the Data Protection Officer, which include: (i) informing the controller, processor and their relevant employees who process data of their obligations under the GDPR; (ii) monitoring compliance with the GDPR, national data protection legislation and internal policies in relation to the processing of personal data including internal audits; (iii) advising on data protection impact assessments and the training of staff; and (iv) co-operating with the data protection authority and acting as the authority's primary contact point for issues related to data processing.

**7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?**

Yes, the controller or processor must notify the data protection authority of the contact details of the designated Data Protection Officer.

**7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?**

The Data Protection Officer does not necessarily need to be named in the public-facing privacy notice. However, the contact details of the Data Protection Officer must be notified to the data subject when personal data relating to that data subject are collected. As a matter of good practice, the Article 29 Working Party (the "**WP29**") (now the European Data Protection Board (the "**EDPB**")) recommended in its 2017 guidance on Data Protection Officers that both the data protection authority and employees should be notified of the name and contact details of the Data Protection Officer.

## 8 Appointment of Processors

**8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?**

Yes. The business that appoints a processor to process personal

data on its behalf, is required to enter into an agreement with the processor which sets out the subject matter for processing, the duration of processing, the nature and purpose of processing, the types of personal data and categories of data subjects and the obligations and rights of the controller (i.e., the business).

It is essential that the processor appointed by the business complies with the GDPR.

**8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?**

The processor must be appointed under a binding agreement in writing. The contractual terms must stipulate that the processor: (i) only acts on the documented instructions of the controller; (ii) imposes confidentiality obligations on all employees; (iii) ensures the security of personal data that it processes; (iv) abides by the rules regarding the appointment of sub-processors; (v) implements measures to assist the controller with guaranteeing the rights of data subjects; (vi) assists the controller in obtaining approval from the relevant data protection authority; (vii) either returns or destroys the personal data at the end of the relationship (except as required by EU or Member State law); and (viii) provides the controller with all information necessary to demonstrate compliance with the GDPR.

## 9 Marketing

**9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).**

Marketing communications are covered by Article 106 of the Regulation of Electronic Communications and Post Law N.112(I)/2004. The prior free and informed consent of the data subject is required, except where the data subject is an existing customer of the data controller and the marketing communications relate to the promotion of goods or services similar to those already received from the data subject by the data controller, in which case direct marketing is allowed provided that the data subject is given the opportunity to opt out, free of charge and easily. This concerns the use of automated calling and communications systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail, for the purposes of direct marketing.

**9.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?**

Article 106 of the Law regulates direct marketing to natural persons. Based on The Order on the Legal Persons (Safeguarding of Legitimate Interests concerning Unsolicited Communications) of 2005 (the "**Order**"), issued by the Commissioner for Electronic Communications and Mail Regulation, the protection against unsolicited communications has also been extended to legal entities (companies).

Article 4 of the Order provides that the use of automated dialling systems from a person without human intervention (automatic dialling machines) or facsimile (fax) devices for direct marketing calls to subscribers shall be permitted where such subscribers:

(a) have stated that they accept such calls from another person through their subscriber line;
(b) have stated in the Cyprus Phonebook Database that they wish to receive such calls from that person; or
(c) have indicated to the person who has assigned the telephone numbers that they wish to receive such calls to such telephone numbers.

Those persons stated in Article 4 (a) and (c) have an obligation to explicitly request the consent of the subscriber, which shall be obtained in printed and electronic form.

Article 5 of the Order provides that the use of public electronic communications networks by a person for the purpose of sending e-mails and/or sending SMS messages for the purpose of direct marketing to subscribers shall be authorised in cases where such subscribers have:

(a) stated that they wish to receive such messages from that person;
(b) stated in the Cyprus Phonebook Database that they wish to receive such messages; or
(c) indicated to the person providing their email and/or SMS services that they wish to receive such messages.

Those persons stated in Article 5 (a) and (c) have an obligation to explicitly request the consent of the subscriber, which shall be obtained in printed and electronic form.

**9.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).**

See questions 9.1 and 9.2.

Unsolicited communications for the purpose of direct marketing by means other than those provided for in questions 9.1 and 9.2 shall not be permitted without the prior consent of the subscribers concerned.

**9.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?**

This is not applicable.

**9.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?**

Yes. The Commissioner has, since 2005, dealt with 11 cases of marketing restriction violations. The fines imposed vary within the range of €400–€8,000 by mitigating and aggravating factors, such as whether the violation was a one-off incident or was repetitive, whether the perpetrator immediately admitted to a breach, whether the number of complainants was small or large, and whether measures to avoid future breach of the law were taken or not and if this influenced the Commissioner's decision on the sanction to be imposed.

Some of the most recent administrative penalties imposed by the Commissioner for a violation of section 106 of Law N.112(I)/2004 are the following:

- Fine against a pizza shop due to the sending of marketing messages without allowing the addressee to stop receiving the messages in an easy way (€1,000).
- Fine against an e-commerce website due to the sending of marketing messages even after the complainants had unsubscribed from receiving marketing material. The data

controller had at the time changed the email marketing platform (€3,400).

- Fine against an insurance company. The company had been sending marketing material without the consent of the data subjects and without having a prior business relationship with them. The Commissioner decided that telephone numbers, even if selected randomly, are personal data if the phone number holder can be easily identified (€4,000).

See also sanctions and fines below in question 16.3.

**9.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?**

This issue has been dealt with by the Commissioner, who has issued fines against unlawful data processing for marketing purposes by various candidates during political elections. The Commissioner has issued the following guidance:

> "[C]andidates should provide a list of the recipients' numbers or addresses. If advertisers maintain their own list, they must be able to ensure that they have received the consent of the recipients with regard to the particular type of advertising requested by the candidate (e.g. the recipients have stated that they are interested in receiving political messages from anyone). In messages sent, it should be clear who the advertiser is who has sent the messages on behalf of the candidate. The above details must be provided in a contract between the candidate and the advertising company, which has the status of data processor."

The Commissioner also recommended that the data controllers should avoid the use of marketing lists when the legal basis, circumstances of data collection and consent are unknown to the controller. A relevant opinion is uploaded on the Commissioner's website.

**9.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?**

Law N.112(I)/2004 (which implements Directive 2002/58/EC) refers to the power of the Data Protection Commissioner to impose fines in accordance with the Cyprus Data Protection Law. Therefore, the Commissioner is entitled to impose penalties within the maximum level provided in the GDPR and in accordance with the relevant provisions of L.125(I)/2018.

## 10 Cookies

**10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).**

Law N.112(I)/2004, with its amendment in 2012, implements Article 5 of the EU ePrivacy Directive (2009/136/EC). Pursuant to Article 5 of the ePrivacy Directive, the storage of cookies (or other data) on an end user's device requires prior consent (the applicable standard of consent is derived from the GDPR).

This does not apply if: (i) the cookie is for the sole purpose of carrying out the transmission of a communication over an electronic communications network; or (ii) the cookie is strictly necessary to provide an "information society service" (e.g., a service over the internet) requested by the subscriber or user, which means that it must be essential to fulfil their request.

For consent to be valid, it must be informed, specific, freely given and must constitute a real and unambiguous indication of the individual's wishes.

**10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?**

See question 10.1.

**10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?**

On 4 June 2021, the Office of the Data Protection Commissioner announced that as of 22 June 2021 it will start conducting audits on websites that use cookies. However, at the time of writing, the audit results and/or decisions from this enforcement action are not yet known.

**10.4 What are the maximum penalties for breaches of applicable cookie restrictions?**

See question 9.7.

## 11 Restrictions on International Data Transfers

**11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.**

Data transfers to other jurisdictions that are not within the European Economic Area (the "**EEA**") can only take place if the transfer is to an "Adequate Jurisdiction" (as specified by the EU Commission), the business has implemented one of the required safeguards as specified by the GDPR, or one of the derogations specified in the GDPR applies to the relevant transfer. The EDPB Guidelines (2/2018) set out that a "layered approach" should be taken with respect to these transfer mechanisms. If the transfer is not to an Adequate Jurisdiction, the data exporter should first explore the possibility of implementing one of the safeguards provided for in the GDPR before relying on a derogation.

For restrictions on transfers of special categories of data, see question 11.3.

**11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).**

When transferring personal data to a country other than an Adequate Jurisdiction, businesses must ensure that there are appropriate safeguards on the data transfer, as prescribed by the GDPR. The GDPR offers a number of ways to ensure compliance for international data transfers, of which one is consent of the relevant data subject. Other common options are the use of Standard Contractual Clauses or Binding Corporate Rules ("**BCRs**").

Businesses can adopt the Standard Contractual Clauses drafted by the EU Commission – these are available for transfers between controllers, and transfers between a controller (as exporter) and a processor (as importer). International data transfers may also take place on the basis of contracts agreed between the data exporter and data importer provided that they conform

to the protections outlined in the GDPR, and they have prior approval by the relevant data protection authority.

International data transfers within a group of businesses can be safeguarded by the implementation of BCRs. The BCRs will always need approval from the relevant data protection authority. Most importantly, the BCRs will need to include a mechanism to ensure they are legally binding and enforced by every member in the group of businesses. Among other things, the BCRs must set out the group structure of the businesses, the proposed data transfers and their purpose, the rights of data subjects, the mechanisms that will be implemented to ensure compliance with the GDPR and the relevant complainant procedures.

**11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.**

L.125(I)/2018 PART VII provides that when the controller or the processor intends to transfer special categories of personal data to a third country or to an international organisation on the basis of the appropriate safeguards provided for in Article 46, or on the basis of the BCR provided for in Article 47 of the GDPR, the Commissioner must be informed of their intention before transferring such data. Also, a transfer carried out by a controller or processor, of special categories of personal data to a third country or an international organisation, which is based on derogations for specific situations provided for in Article 49 of the GDPR, requires an impact assessment to be undertaken, as well as prior consultation with the Commissioner.

**11.4 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?**

The EDPB has issued Recommendations 01/2020 on supplementary protections to be implemented where appropriate, in respect of transfers made under Standard Contractual Clauses, in light of the *Schrems II* decision. The Commissioner has urged the organisations to follow the guidance from the EDPB.

**11.5 What guidance (if any) has/have the data protection authority(ies) issued in relation to the European Commission's revised Standard Contractual Clauses?**

The EDPB and the European Data Protection Supervisor have issued Joint Opinion 1/2021 in relation to the revised Standard Contractual Clauses. On 4 June 2021, the European Commission published the new SCCs. The Commissioner has urged the organisations to follow the above-mentioned and other relevant guidance from the EDPB.

## 12 Whistle-blower Hotlines

**12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?**

Internal whistle-blowing schemes are generally established in pursuance of a concern to implement proper corporate governance principles in the daily functioning of businesses. Whistle-blowing is designed as an additional mechanism for employees to report misconduct internally through a specific channel and supplements a business' regular information and reporting channels, such as employee representatives, line management, quality-control personnel or internal auditors who are employed precisely to report such misconducts.

The WP29 has limited its Opinion 1/2006 on the application of EU data protection rules to internal whistle-blowing schemes to the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime. The scope of corporate whistle-blower hotlines, however, does not need to be limited to any particular issues. In the Opinion, it is recommended that the business responsible for the whistle-blowing scheme should carefully assess whether it might be appropriate to limit the number of persons eligible for reporting alleged misconduct through the whistle-blowing scheme and whether it might be appropriate to limit the number of persons who may be reported through the scheme, in particular in the light of the seriousness of the alleged offences reported.

While participating in the International Panel Event about the new European Directive to protect Whistle-blowers on 10 February 2020, the Commissioner made the following points:

- The Office of the Commissioner, as part of the consultation which it provided on several occasions for legislative initiatives (such as the transparency in the process of public decision-making draft Law, and a package of laws regarding the reporting of corruption acts), has made the following recommendations:
  - There should be one comprehensive legislation instead of fragmented provisions in different legislations.
  - The comprehensive legislation should be aligned with the proposed Directive.
  - It should cover whistleblowing in both the public and the private sector.
  - It should establish procedures, channels and mechanisms for the lawful submission, handling and monitoring of reported whistleblowing and for the protection of personal data.
  - The whistle-blower's identity should be protected but it should be subject to conditions.
  - For example, a whistle-blower's identity should be disclosed to regulatory or prosecuting authorities, when this is necessary for the performance of their duties.
- In the frame of the National Strategy Against Corruption (a national anti-corruption action plan), the Commissioner's office has appointed two Officers since June 2019 to participate in the activities and training programmes envisaged in the action plan.
- Cyprus must transpose the provisions of the Directive (EU) 2019/1937 into national legislation by December 2021.

**12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?**

Anonymous reporting is not prohibited under EU data protection law; however, it raises problems as regards the essential requirement that personal data should only be collected fairly. In Opinion 1/2006, the WP29 considered that only identified

reports should be advertised in order to satisfy this requirement. Businesses should *not* encourage or advertise the fact that anonymous reports may be made through a whistle-blower scheme.

An individual who intends to report to a whistle-blowing system should be aware that he/she will not suffer due to his/her action. The whistle-blower, at the time of establishing the first contact with the scheme, should be informed that his/her identity will be kept confidential at all the stages of the process, and in particular will not be disclosed to third parties, such as the incriminated person or to the employee's line management. If, despite this information, the person reporting to the scheme still wants to remain anonymous, the report will be accepted into the scheme. Whistle-blowers should be informed that their identity may need to be disclosed to the relevant people involved in any further investigation or subsequent judicial proceedings instigated as a result of any enquiry conducted by the whistle-blowing scheme.

See also question 12.1.

## 13 CCTV

### 13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

A data protection impact assessment ("**DPIA**") must be undertaken with assistance from the Data Protection Officer when there is systematic monitoring of a publicly accessible area on a large scale. If the DPIA suggests that the processing would result in a high risk to the rights and freedoms of individuals prior to any action being taken by the controller, the controller must consult the data protection authority.

During the course of a consultation, the controller must provide information on the responsibilities of the controller and/or processors involved, the purpose of the intended processing, a copy of the DPIA, the safeguards provided by the GDPR to protect the rights and freedoms of data subjects and where applicable, the contact details of the Data Protection Officer.

If the data protection authority is of the opinion that the CCTV monitoring would infringe the GDPR, it has to provide written advice to the controller within eight weeks of the request of a consultation and can use any of its wider investigative, advisory and corrective powers outlined in the GDPR.

The Commissioner has issued specific Guidance on the use of CCTV and has recently emphasised the necessity for organisations and businesses to conduct a DPIA in accordance with Article 35 of the GDPR.

### 13.2 Are there limits on the purposes for which CCTV data may be used?

Based on a Commissioner's decision, "the recording of audio (conversations) data through the CCTV system is considered to be highly intrusive to individuals' privacy, infringes human dignity and is generally banned in all cases".

Furthermore, the Commissioner has issued a relevant Announcement regarding the "installation of Closed-Circuit Video Surveillance (CCTV) in publicly accessible areas". The commissioner has stated the following examples:

Examples where capturing images using CCTV is allowed:

- By a building entrance/exit.
- Outside an elevator, focusing solely on it.
- Above a card/cash machine, focusing solely on it.
- Parking lot.

Examples where capturing images using CCTV is not allowed:

- Corridors.
- Inside an elevator.
- In a waiting area.
- Bathrooms.
- Indoor/outdoor dining area, cafeteria, restaurant, etc.

In addition, the Commissioner has stated that the installation of CCTV in private areas (such as houses/condominiums) for processing by a natural person related to personal or household activities does not fall within the scope of the legislation on the protection of personal data. However, the recording range of the CCTV should not exceed the scope of the private space. In apartments, the use of CCTV by a tenant should not affect the privacy of other tenants or the public. If the CCTV is to be installed by the building's management committee, it should be restricted to shared areas following the decision of the tenants that comply with the provisions of the committee's Memorandum.

## 14 Employee Monitoring

### 14.1 What types of employee monitoring are permitted (if any), and in what circumstances?

Regardless of the type of employee monitoring, the Commissioner's decisions clarify that the employer must be able to justify the lawfulness and necessity of control and monitoring, and that there is no other less intrusive method for carrying out the objectives pursued. The legitimate interest invoked by the employer must prevail over the rights, interests, and fundamental freedoms of employees. Furthermore, all the other data protection principles must always be respected.

One monitoring method has been decided to be disproportional both by the Commissioner and the Supreme Court: biometric data (i.e., fingerprints) in the workplace. In summary, the Court and the Commissioner have ruled that the use of biometric data to monitor employees at work appear to go against the principles of proportionality and lawfulness of processing of personal data. The Commissioner's decisions and guidance are interesting in the sense that it clarifies that: a) such processing would only be proportional and lawful only in situations where, exceptionally, the use of a system could be justified, solely for reasons of site security, in the case of emergency/high security (such as ports, airports, military facilities); and b) even in the case where the controller has obtained the consent of the persons whose biometric data will be processed, this consent does not legitimise the processing.

### 14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Employers must in all cases inform the employees about the purpose, manner and duration of control and monitoring they intend to apply prior to the beginning of the monitoring. It is good practice for the employer to adopt a written policy for determining the parameters of telephone use, computers, internet, other electronic means of communication and material/equipment of the company/organisation of employees, and ways/systems through which the employer will monitor/control their use. Secret surveillance or monitoring of employees is never permitted, as employees must be notified in advance.

Directives from the Commissioner suggest avoiding consent as a legal basis for processing employees' data, due to the imbalance of power between the employer and the employees, which might render the consent in question not freely given or unambiguous.

The control and monitoring of employees in the workplace is permitted by law only when the employer is able to justify and be accountable for the lawfulness and necessity of such control and monitoring and when there is no other less intrusive way of achieving the purposes he/she seeks.

Furthermore, the Commissioner has issued a relevant Opinion regarding the "installation of Closed-Circuit Video Surveillance (CCTV) in the workplace and the use of biometric data". Among other suggestions, the Commissioner's guidance regarding monitoring using CCTV is the following:

- The use of the CCTV could be justified in special and exceptional cases where this is justified by the nature and work conditions and is necessary to protect the health and safety of workers or to protect critical workplaces (e.g., the military, banks, high-risk facilities). In a typical business office space, video surveillance should be restricted to entry and exit areas, outside elevators, stairways, parking, cashiers or safes, electromechanical equipment, etc., provided that the cameras are focused on the good which they protect and not on the workers' places and their faces. It is forbidden to register employees in their offices, meeting rooms, corridors, kitchens, outside toilets, changing rooms, etc.

**14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?**

According to the Commissioner's guidelines, it is good practice for employers to consult employee representatives and trade unions prior to the installation and use of control measures within the workplace.

## 15 Data Security and Data Breach

**15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?**

Yes. Personal data must be processed in a way which ensures security and safeguards against unauthorised or unlawful processing, accidental loss, destruction and damage of the data.

Both controllers and processors must ensure they have appropriate technical and organisational measures to meet the requirements of the GDPR. Depending on the security risk, this may include: the encryption of personal data; the ability to ensure the ongoing confidentiality, integrity and resilience of processing systems; an ability to restore access to data following a technical or physical incident; and a process for regularly testing and evaluating the technical and organisation measures for ensuring the security of processing.

**15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

The controller is responsible for reporting a personal data breach without undue delay (and in any case within 72 hours of first becoming aware of the breach) to the relevant data protection authority, unless the breach is unlikely to result in a risk to the rights and freedoms of the data subject(s). A processor must notify any data breach to the controller without undue delay.

The notification must include the nature of the personal data breach including the categories and number of data subjects concerned, the name and contact details of the Data Protection Officer or relevant point of contact, the likely consequences of the breach and the measures taken to address the breach including attempts to mitigate possible adverse effects.

**15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

Controllers have a legal requirement to communicate the breach to the data subject, without undue delay, if the breach is likely to result in a high risk to the rights and freedoms of the data subject.

The notification must include the name and contact details of the Data Protection Officer (or point of contact), the likely consequences of the breach and any measures taken to remedy or mitigate the breach.

The controller may be exempt from notifying the data subject if the risk of harm is remote (e.g., because the affected data is encrypted), the controller has taken measures to minimise the risk of harm (e.g., suspending affected accounts) or the notification requires a disproportionate effort (e.g., a public notice of the breach).

**15.4 What are the maximum penalties for data security breaches?**

The maximum penalty is the higher of €20 million or 4% of worldwide turnover.

## 16 Enforcement and Sanctions

### 16.1 Describe the enforcement powers of the data protection authority(ies).

| Investigatory / Enforcement Power | Civil/Administrative Sanction | Criminal Sanction |
|---|---|---|
| Investigative Powers | The Commissioner:<br>■ may not investigate a complaint or discontinue its investigation for reasons of public interest and shall notify to the data subject, within a reasonable period, of the reasons for doing so;<br>■ shall have access to all the personal data and to all the information required for the performance of his or her tasks and the exercise of his or her powers, including confidential information, except for information covered by legal professional privilege;<br>■ shall have the power to enter, without necessarily informing the controller or the processor or their representative in advance, any office, professional premises or mean of transport, with the exception of residences; and<br>■ for the exercise of the investigative powers, the Commissioner may:<br>■ be assisted by an expert or/and the police; and<br>■ seize documents or electronic equipment by virtue of a search warrant in accordance with the Criminal Procedure Law. | The Commissioner shall notify to the AG of the Republic and/or to the police any contravention of the provisions of the GDPR or of the L.125(I)2018, that may constitute an offence in accordance with Section 33 of L.125(I)2018 provisions below.<br>1. If a person is convicted for committing any of the following offences, he or she shall be subject to imprisonment which shall not exceed three years or a fine which shall not exceed €30,000 or to both of these penalties:<br>■ a controller or a processor who does not maintain the record of processing activities as per Article 30 of the GDPR or provides false, inaccurate, incomplete or misleading information to the Commissioner in relation to this record;<br>■ a controller or a processor who does not cooperate with the Commissioner in the performance of its tasks;<br>■ a controller who does not notify to the Commissioner a personal data breach, in accordance with the provisions of Article 33 (1) of the GDPR; or, in the case of a processor, in accordance with the provisions Article 33 (2), paragraph 2 of the GDPR;<br>■ a controller who does not communicate a personal data breach to the data subject, in accordance with Article 34 of the GDPR;<br>■ a controller who does not carry out an impact assessment, in breach of Article 35 (1) of the GDPR or of L.125(I)2018;<br>■ a controller or a processor who prevents the DPO from performing his or her tasks;*<br><br>**Contd. overleaf** |
| Corrective Powers | ■ The Commissioner shall require the Cyprus Organization for the Promotion of Quality to revoke the accreditation of a certification body, when the Commissioner ascertains that the requirements for the certification are not or are no longer met or where actions taken by the certification body violate the provisions of the Regulation or of L.125(1)2018.<br>■ The Commissioner shall denounce the Cyprus Organization for the Promotion of Quality to the European Commission, in the event the organisation does not revoke an accreditation of a certification body in accordance with L.125(I)2018. | |
| Authorisation and Advisory Powers | ■ The Commissioner may publish on the Office's website the means of lodging complaints and requests, and shall examine a complaint and, where possible, depending on the nature and type of the complaint, shall inform the complainant in writing of the progress and outcome within 30 days of the submission of the complaint.<br>■ The Commissioner shall inform, where appropriate, the data subject, the controller and the processor of the time limits provided for in Articles 60 to 66 of the GDPR.<br>■ The Commissioner may establish and make public the list of processing operations and cases that require the designation of a DPO. | |

| Investigatory / Enforcement Power | Civil/Administrative Sanction | Criminal Sanction |
|---|---|---|
| Authorisation and Advisory Powers ctd. | ■ In addition to the authorisation and advisory powers provided for in the GDPR, the Commissioner shall have the power to:<br>■ authorise the combination of filing systems in accordance with L.125(I)2018 and impose terms and conditions for the materialisation of the combination;<br>■ impose terms and conditions in relation to the application of the measures for the restriction of the rights referred to in section 11 of this Law;<br>■ impose terms and conditions for the exemption to the obligation to communicate the data breach;<br>■ impose explicit limits for the transfer of special categories of personal data;<br>■ recommend to the Minister of Justice and Public Order the conclusion of agreements with other countries and conclude, establish and sign the Memoranda of Understanding provided for in L.125(I)2018; and<br>■ notify to the Attorney General of the Republic and/or to the police any contravention of the provisions of the Regulation or of this law, that may constitute an offence in accordance with provisions of section 33 of this Law. | ■ a certification body which issues or does not withdraw a certification, in accordance with the provisions of Article 42 of the GDPR;<br>■ a controller or a processor who transfers personal data to a third country or an international organisation, in breach of Chapter V of the GDPR;<br>■ a controller or a processor who transfers personal data to a third country or an international organisation, in breach of the explicit limits imposed by the Commissioner in accordance with L.125(I)2018;*<br>■ a person who intervenes without the right, in any way, in a filing system or acquires knowledge of the personal data thereof or removes, alters, damages, destroys, processes or uses in any way, discloses, communicates, renders them accessible to non-authorised persons or allows these persons to acquire knowledge of the said data, for gainful purposes or not; or<br>■ a controller or processor who prevents or impairs the exercise of the Commissioner's powers.<br>* If a person is convicted of committing this offence, which damages the interests of the Republic or impairs the free governing of the Republic or compromises national security, he or she shall be subject to imprisonment which shall not exceed five years, or to a fine which shall not exceed €50,000, or to both of these penalties.<br>2. If a person is convicted for committing any of the following offences, he or she shall be subject to imprisonment which shall not exceed one year, or to a fine which shall not exceed €10,000 or to both of these penalties:<br>■ a controller or a processor who does not comply with the GDPR and L.125(I)2018 when carrying out a processing activity which does not constitute an offence in accordance with the provisions of this section; or<br>■ a public authority or body which proceeds to the combination of large-scale filing systems in breach of L.125(I)2018.<br>Where the controller or the processor is an enterprise or a group of undertakings, the legal responsibility lies with the person designated as the supreme executive instrument or body of the enterprise or group of undertakings.<br>Where the controller or the processor is a public authority or body, the legal responsibility lies with the head of the public authority or body, or with the person who exercises substantial administration of the public authority or body. |
| Imposition of administrative fines for infringements of specified GDPR provisions | The GDPR provides for administrative fines which can be €20 million or up to 4% of the business' worldwide annual turnover of the preceding financial year.<br>■ Where the administrative fine remains unpaid, it shall be collected as a civil debt due to the Republic.<br>■ An administrative fine imposed on a public authority or body, which relates to non-profitable activities, shall not exceed €200,000. | |
| Non-compliance with a data protection authority | The GDPR provides for administrative fines which will be €20 million or up to 4% of the business' worldwide annual turnover of the preceding financial year, whichever is higher. | |

**16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?**

The GDPR entitles the relevant data protection authority to impose a temporary or definitive limitation including a ban on processing.

**16.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.**

The Commissioner's Office has provided organisations and businesses with sufficient information and presentations regarding the necessary steps for compliance, prior to May 2018 (the GDPR enforcement date). Since then, the Commissioner's Office has identified the following as the main areas of non-compliance, either by responding to complaints or on its own initiative:

- Failure to keep and maintain a Record of Processing Activities as per Article 30 of the GDPR.
- Failure and gaps by organisations in providing sufficient information to their DPOs in order to perform their tasks.
- Lack of procedures to implement proper technical and organisational measures, or to apply easy and free ways of unsubscribing from direct marketing communications.

Some of the recent cases are the following:

1. Ban and administrative fine on a travel agency concerning the lack of legal basis for the use of the "Bradford Factor" tool, which was used to score the sick leave of employees (€82,000 fine).
2. Administrative fine of €10,000 on the Real Estate Registration Council regarding the non-satisfaction of the complainant's access request and lack of cooperation with the Office of the Commissioner.
3. Administrative fine of €6,000 on a company for the unlawful disclosure of personal data to the Parliamentary Committee in the House of Representatives instead of the anonymised list of buyers of properties under management, and the list of their names.
4. Administrative fine of €40,000 on the Electricity Authority of Cyprus concerning the wrong legal basis for the use of the "Bradford Factor" tool.
5. Administrative fine of €25,000 on the Hellenic Bank regarding the delay found in relation to the Bank's obligation to notify a security incident to the Office of the Commissioner as well as the breach of the principle of data availability of files that remained locked inside a vault during the period 2015–2019.
6. Administrative fine of €5,000 against a hospital for loss of a patient's file.
7. Administrative fine of €9,000 against the Social Insurance Services for failure to notify the Commissioner's Office regarding a security incident and for insufficient internal technical and organisational measures.
8. Administrative fine of €10,000 against a newspaper for the unlawful disclosure of names and photographs of police investigators.
9. Administrative fine of €500 against a university for sending SMS messages to a student without providing the ability to stop receiving messages free of charge.

**16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?**

The Commissioner's Office has been the Lead Supervisory Authority for 12 cross-border cooperation cases out of the 416 registered in the system, which concern companies whose main establishment is in Cyprus.

## 17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

**17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?**

Typically, companies are expected to follow three main steps when dealing with such requests: 1) determine whether there is a legal framework in place which would allow the disclosure i.e. the litigation procedural rules of Cyprus, international conventions/treaties (e.g. Hague convention), bilateral or other agreements, which compel such cooperation with the foreign country's rules); 2) consider the scope and type of the request and justify the disclosure under GDPR and the Cyprus Data Protection Law 125(I)2018 from a data protection law perspective including any restrictions regarding data transfers to third countries; and 3) apply security measures on document/data disclosure in order to protect the personal data included thereof (i.e. pseudonymisation/redaction).

In relation to steps 1 and 2, GDPR Article 48 provides that "Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter (meaning GDPR Chapter V)".

**17.2 What guidance has/have the data protection authority(ies) issued?**

There is no standalone guidance by the Commissioner's office. Companies should consult the Art.29 Working Document 1/2009 on pre-trial discovery for cross-border civil litigation.

## 18 Trends and Developments

**18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.**

During 2021, the Commissioner's Office conducted audits, through audit questionnaires. Also, the Office has inevitably turned its focus on issuing relevant guidance for sectors which have been heavily affected by the COVID-19 pandemic, such as education, healthcare, and employment.

The Commissioner's Office has been interested in investigating the compliance practices of many organisations both in the private and public sector, sometimes with the help of private independent security consultants.

Also, the Commissioner's Office – whilst maintaining its enforcement and data protection authority role – has been seeking to raise awareness and assist DPOs by answering as many relevant questions as possible. The focus of enforcement action remains on high-risk industries and practices such as hospitals, financial institutions, schools, insurance companies and marketing.

### 18.2 What "hot topics" are currently a focus for the data protection regulator?

The Commissioner's Office is always monitoring the trends and technological advances such as Blockchain, artificial intelligence, FinTech, AdTech and the Internet of Things. The Commissioner's Office is aware of the potential privacy implications arising from the use of such technologies and is continuously observing the relevant EU legislation and guidance for more updates.

Also, vey recently the Cabinet passed the law establishing the Deputy Ministry for Research, Innovation and Digital Policy, which was set up to promote the government's digital agenda. This is considered an important stepping stone towards creating the foundation for legislative and government initiatives in the field of innovation. Specifically, the use of blockchain technology is expected to be regulated in 2021.

**Loizos Papacharalambous** has been a member of the Cyprus Bar Association since 2004. He graduated from the University of Bristol before going on to successfully complete the Bar Vocational Course, becoming a member of Gray's Inn. In 2006, Loizos successfully completed the International and Comparative Commercial Arbitration Diploma with Queen Mary University of London. In 2011, Loizos was admitted as a Member of the Chartered Institute of Arbitrators. Loizos is currently attending courses to obtain an M.Sc. in Finance and Banking. His main areas of practice are commercial and corporate litigation and representation of banks, investment and insurance companies.
Loizos has been the Vice-Chairman of the Cyprus Telecommunications Authority (CYTA), the Vice-President of the Nicosia Bar Association and the Chairman of the Housing Finance Corporation.

**Koushos Korfiotis Papacharalambous LLC**
20 Costi Palama str.
Aspelia Court
1096 Nicosia
Cyprus

Tel: +357 22 664 555
Email: loizosp@kkplaw.com
URL: www.kkplaw.com

**Anastasios Kareklas** is a lawyer at Koushos Korfiotis Papacharalambous LLC, with wide-ranging knowledge and experience on ICT law, with a particular focus on Data Protection Law and e-Commerce Law. Anastasios holds an LL.B. (Hons) from the University of Sussex and an LL.M. in Computer and Communications Law from Queen Mary University of London (QMUL). Anastasios is a Certified Information Privacy Professional (CIPP/E) by the International Association of Privacy Professionals (IAPP), acts as Data Protection Officer and is a key member of the Data Protection Team at KKP LLC. He provides consultation on compliance issues and legal advice on data protection and privacy.

**Koushos Korfiotis Papacharalambous LLC**
20 Costi Palama str.
Aspelia Court
1096 Nicosia
Cyprus

Tel: +357 22 664 555
Email: akareklas@kkplaw.com
URL: www.kkplaw.com

Koushos Korfiotis Papacharalambous LLC (KKP LLC) comprises more than 20 lawyers based in our offices in Nicosia. KKP LLC is a full-service law firm with an industry focus on financial services including financial, insurance and banking institutions, intellectual property, data protection & privacy, real estate and construction, corporate and securities law. The firm operates in multi-disciplinary teams, which allows us to provide clients with individualised and expert advice. Our team of lawyers has more than 30 years of experience, combining an extensive knowledge of the Cypriot legal system with an in-depth understanding of international and European law. Partners of the firm are members of professional legal organisations such as the International Trademark Association (INTA), the European Communities Trade Mark Association (ECTA), MARQUES, the Pharmaceutical Trade Marks Group (PTMG), the International Tax Planning Association, and the Chartered Institute of Arbitrators, while a number of them are also endorsed and highly rated by the world's leading international legal directories, including *The Legal 500*.

**www.kkplaw.com**

KKP
KOUSHOS KORFIOTIS PAPACHARALAMBOUS LLC
ADVOCATES & LEGAL CONSULTANTS

# Denmark


Heidi Højmark Helveg


Niels Dahl-Nielsen

CO:PLAY Advokatpartnerselskab

## 1 Relevant Legislation and Competent Authorities

### 1.1 What is the principal data protection legislation?

Since 25 May 2018, the principal data protection legislation in the EU has been Regulation (EU) 2016/679 (the "**General Data Protection Regulation**" or "**GDPR**"). The GDPR repealed Directive 95/46/EC (the "**Data Protection Directive**") and has led to increased (though not total) harmonisation of data protection law across the EU Member States.

### 1.2 Is there any other general legislation that impacts data protection?

On 23 May 2018, the Act on supplementary provisions to the regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the "**Data Protection Act**" or the "**DP Act**") was adopted and enforced.

Executive Order of 9 December 2011 (the "**Cookie Order**") implements the ePrivacy Directive 2002/58/EC (as amended by Directive 2009/136/EC) (the "**ePrivacy Directive**"), which provides a specific set of privacy rules to harmonise the processing of personal data by the telecoms sector. In January 2017, the European Commission published a proposal for an ePrivacy regulation (the "**ePrivacy Regulation**") that would harmonise the applicable rules across the EU. In September 2017, the Council of the European Union published proposed revisions to the draft. In March 2021, the Council has finally agreed on a draft of the future ePrivacy Regulation and will start negotiations with the EU Parliament.

Act no. 128 on Electronic Communications Networks and Services of 7 February 2014 (the "**Tele Act**") and Executive Order on the retention and storage of traffic data by providers of electronic communications networks and services, no. 988 of 28 September 2006, as amended by executive order of amendment no. 660 of 19 June 2014 (the "**Retention Order**"), implement parts of Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

### 1.3 Is there any sector-specific legislation that impacts data protection?

Yes, there is sector-specific data protection regulation in the following sectors:

- the health sector;
- the telecommunications sector;
- the financial sector; and
- the criminal enforcement field.

### 1.4 What authority(ies) are responsible for data protection?

Principally, the Danish Data Protection Agency (the "**DPA**") is the supervisory authority with responsibility for compliance with the GDPR and the DP Act.

The **Danish Court Administration** supervises the processing of data carried out for the courts when they do not act in their capacity of courts.

The **Danish Business Authority** is the supervisory authority for the regulation of cookies and telecommunications.

## 2 Definitions

### 2.1 Please provide the key definitions used in the relevant legislation:

- "**Personal Data**"
  Any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- "**Processing**"
  Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- "**Controller**"
  The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- "**Processor**"
  A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

- "**Data Subject**"
  An individual who is the subject of the relevant personal data.
- "**Sensitive Personal Data**"
  Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health or sex life and sexual orientation, genetic data or biometric data.
- "**Data Breach**"
  A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
- "**Pseudonymous Data**"
  Data that are indicated as a code but can be personally identifiable by using additional information and are therefore personal data covered by the GDPR.

## 3 Territorial Scope

### 3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The GDPR applies to businesses that are established in any EU Member State, and that process personal data (either as a controller or processor, and regardless of whether or not the processing takes place in the EU) in the context of that establishment.

A business that is not established in any Member State, but is subject to the laws of a Member State by virtue of public international law, is also subject to the GDPR.

The GDPR applies to businesses outside the EU if they (either as controller or processor) process the personal data of EU residents in relation to: (i) the offering of goods or services (whether or not in return for payment) to EU residents; or (ii) the monitoring of the behaviour of EU residents (to the extent that such behaviour takes place in the EU).

Further, the GDPR applies to businesses established outside the EU if they monitor the behaviour of EU residents (to the extent such behaviour takes place in the EU).

## 4 Key Principles

### 4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  Personal data must be processed lawfully, fairly and in a transparent manner. Controllers must provide certain minimum information to data subjects regarding the collection and further processing of their personal data. Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
- **Lawful basis for processing**
  Processing of personal data is lawful only if, and to the extent that, it is permitted under EU data protection law. The GDPR provides an exhaustive list of legal bases on which personal data may be processed, of which the following are the most relevant for businesses: (i) prior, freely given, specific, informed and unambiguous consent of the data subject; (ii) contractual necessity (i.e., the processing is necessary for the performance of a contract to which the data subject is a party, or for the purposes of pre-contractual measures taken at the data subject's request); (iii) compliance with legal obligations (i.e., the controller has a legal obligation, under the laws of the EU or an EU Member State, to perform the relevant processing); or (iv) legitimate interests (i.e., the processing is necessary for the purposes of legitimate interests pursued by the controller, except where the controller's interests are overridden by the interests, fundamental rights or freedoms of the affected data subjects).
  Please note that businesses require stronger grounds to process sensitive personal data. The processing of sensitive personal data is only permitted under certain conditions, of which the most relevant for businesses are: (i) explicit consent of the affected data subject; (ii) the processing is necessary in the context of employment law; or (iii) the processing is necessary for the establishment, exercise or defence of legal claims.
- **Purpose limitation**
  Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes. If a controller wishes to use the relevant personal data in a manner that is incompatible with the purposes for which they were initially collected, it must: (i) inform the data subject of such new processing; and (ii) be able to rely on a lawful basis as set out above.
- **Data minimisation**
  Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed. A business should only process the personal data that it actually needs to process in order to achieve its processing purposes.
- **Proportionality**
  Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes.
- **Retention**
  Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- **Accuracy**
  Personal data must be accurate and, where necessary, kept up to date. A business must take every reasonable step to ensure that personal data that are inaccurate are either erased or rectified without delay.
- **Data security**
  Personal data must be processed in a manner that ensures appropriate security of those data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- **Accountability**
  The controller is responsible for, and must be able to demonstrate, compliance with the data protection principles set out above.

## 5 Individual Rights

### 5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**
  A data subject has the right to obtain from a controller the following information in respect of the data subject's personal data: (i) confirmation of whether, and where, the controller is processing the data subject's personal data; (ii)

information about the purposes of the processing; (iii) information about the categories of data being processed; (iv) information about the categories of recipients with whom the data may be shared; (v) information about the period for which the data will be stored (or the criteria used to determine that period); (vi) information about the existence of the rights to erasure, to rectification, to restriction of processing and the objection of processing; (vii) information about the existence of the right to complain to the relevant data protection authority; (viii) where the data were not collected from the data subject, information as to the source of the data; and (ix) information about the existence of, and an explanation of the logic involved in, any automated processing that has a significant effect on the data subject.

Additionally, the data subject may request a copy of the personal data being processed.

- **Right to rectification of errors**
  Controllers must ensure that inaccurate or incomplete data are erased or rectified. Data subjects have the right to rectification of inaccurate personal data.
- **Right to deletion/right to be forgotten**
  Data subjects have the right to erasure of their personal data (the "right to be forgotten") if: (i) the data are no longer needed for their original purpose (and no new lawful purpose exists); (ii) the lawful basis for the processing is the data subject's consent, the data subject withdraws that consent, and no other lawful ground exists; (iii) the data subject exercises the right to object, and the controller has no overriding grounds for continuing the processing; (iv) the data have been processed unlawfully; or (v) erasure is necessary for compliance with EU law or national data protection law.
- **Right to object to processing**
  Data subjects have the right to object, on grounds relating to their particular situation, to the processing of personal data where the basis for that processing is either public interest or legitimate interest of the controller. The controller must cease such processing unless it demonstrates compelling legitimate grounds for the processing which overrides the interests, rights and freedoms of the relevant data subject or requires the data in order to establish, exercise or defend legal rights.
- **Right to restrict processing**
  Data subjects have the right to restrict the processing of personal data, which means that the data may only be held by the controller, and may only be used for limited purposes if: (i) the accuracy of the data is contested (and only for as long as it takes to verify that accuracy); (ii) the processing is unlawful and the data subject requests restrictions (as opposed to exercising the right to erasure); (iii) the controller no longer needs the data for their original purpose, but the data are still required by the controller to establish, exercise or defend legal rights; or (iv) verification of overriding grounds is pending, in the context of an erasure request.
- **Right to data portability**
  Data subjects have a right to receive a copy of their personal data in a commonly used machine-readable format, and transfer their personal data from one controller to another or have the data transmitted directly between controllers.
- **Right to withdraw consent**
  A data subject has the right to withdraw their consent at any time. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject must be informed of the right to withdraw consent. It must be as easy to withdraw consent as to give it.
- **Right to object to marketing**
  Data subjects have the right to object to the processing of personal data for the purpose of direct marketing, including profiling.
- **Right to complain to the relevant data protection authority(ies)**
  Data subjects have the right to lodge complaints concerning the processing of their personal data with the Danish Data Protection Agency, if the data subjects live in Denmark or the alleged infringement occurred in Denmark.
- **Right to basic information**
  Data subjects have the right to be provided with information on the identity of the controller, the reasons for processing their personal data and other relevant information necessary to ensure the fair and transparent processing of personal data.

## 6 Registration Formalities and Prior Approval

### 6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

According to the DP Act, private data controllers shall obtain an authorisation from the DPA prior to the processing of personal data where the processing of data is carried out:

(i) for the purpose of warning others against having business relations or accepting employment with a certain data subject;
(ii) for the purpose of commercial disclosure of data for the assessment of financial standing and creditworthiness; or
(iii) exclusively for the purpose of operating legal information systems. Amendments also require authorisation.

The DPA will lay down the terms for processing.

According to the Danish Act on information databases operated by the mass media, the mass media shall notify the DPA of editorial information databases and publicly available information databases.

### 6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

The controller shall provide the DPA with specific information on the processing, e.g., "listing all processing activities, categories of data", *cf.* question 6.5.

### 6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

Registrations and notifications are made according to the processing purpose.

### 6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

In very few cases, private controllers have an obligation to notify the DPA and obtain approval prior to processing personal data for specific purposes.

**6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?**

An authorisation application requires information on:

- name and contact details of the controller (including any joint controller, representative and data protection officer);
- purpose and a general description of the processing;
- categories of data subjects;
- categories of personal data;
- categories of recipients;
- where applicable, transfers of personal data to a third country;
- retention period; and
- technical and organisational security measures.

**6.6 What are the sanctions for failure to register/notify where required?**

The provisions on notification of the DPA are based on Article 36, subsection 5 of the GDPR, and the sanctions for non-compliance with the obligation to obtain an authorisation follow the sanction for non-compliance with Article 36, subsection 5.

The purpose of the mass media notification is to exclude the mass media information databases from the scope of the GDPR and DP Act.

There are no sanctions for the mass media's failure to notify the DPA of the information databases. If a mass media organisation fails to notify the DPA, the media's processing of personal data in the information database will be subject to the DP Act and the GDPR.

**6.7 What is the fee per registration/notification (if applicable)?**

There is no registration fee.

**6.8 How frequently must registrations/notifications be renewed (if applicable)?**

Registrations/notifications must be renewed when any amendments are made.

**6.9 Is any prior approval required from the data protection regulator?**

According to the DP Act, prior approval is only required for disclosure of personal data processed for the sole purpose of statistical or scientific studies of significant importance to society, if disclosure to a third party is for: (i) the purpose of processing outside the territorial scope of the GDPR; (ii) processing that relates to biological material; or (iii) the purpose of publication in a recognised scientific journal or similar, *cf.* question 6.1.

**6.10 Can the registration/notification be completed online?**

No, it requires a positive approval from the DPA.

**6.11 Is there a publicly available list of completed registrations/notifications?**

No, but the application and authorisation can be subject to requests of subject access according to the Danish Publicity Act.

**6.12 How long does a typical registration/notification process take?**

It takes a minimum of six months, sometimes longer. There is a very small number of cases at this point.

## 7 Appointment of a Data Protection Officer

**7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.**

The appointment of a Data Protection Officer for controllers or processors is only mandatory in some circumstances, including where there is: (i) large-scale regular and systematic monitoring of individuals; or (ii) large-scale processing of sensitive personal data.

Where a business designates a Data Protection Officer voluntarily, the requirements of the GDPR apply as though the appointment were mandatory.

**7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?**

In the circumstances where appointment of a Data Protection Officer is mandatory, failure to comply may result in the wide range of penalties available under the GDPR.

**7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?**

Yes, and hence the appointed Data Protection Officer should not be dismissed or penalised for performing tasks and should report directly to the highest management level of the controller or processor.

**7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?**

A single Data Protection Officer is permitted by a group of undertakings provided that the Data Protection Officer is easily accessible from each establishment.

**7.5 Please describe any specific qualifications for the Data Protection Officer required by law.**

The Data Protection Officer should be appointed on the basis of professional qualities and should have an expert knowledge of data protection law and practices. While this is not strictly defined, it is clear that the level of expertise required will depend on the circumstances. For example, the involvement of large volumes of sensitive personal data will require a higher level of knowledge.

**7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?**

A Data Protection Officer should be involved in all issues which relate to the protection of personal data. The GDPR outlines the minimum tasks required by the Data Protection Officer, which include: (i) informing the controller, processor and their relevant employees who process data of their obligations under the GDPR; (ii) monitoring compliance with the GDPR, national data protection legislation and internal policies in relation to the processing of personal data including internal audits; (iii) advising on data protection impact assessments and the training of staff; and (iv) co-operating with the data protection authority and acting as the authority's primary contact point for issues related to data processing.

**7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?**

Yes, the controller or processor must notify the data protection authority of the contact details of the designated Data Protection Officer.

**7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?**

The Data Protection Officer does not necessarily need to be named in the public-facing privacy notice. However, the contact details of the Data Protection Officer must be notified to the data subject when personal data relating to that data subject are collected. As a matter of good practice, the Article 29 Working Party (the "**WP29**") (now the European Data Protection Board (the "**EDPB**")) recommended in its 2017 guidance on Data Protection Officers that both the data protection authority and employees should be notified of the name and contact details of the Data Protection Officer.

## 8 Appointment of Processors

**8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?**

Yes. The business that appoints a processor to process personal data on its behalf, is required to enter into an agreement with the processor which sets out the subject matter for processing, the duration of processing, the nature and purpose of processing, the types of personal data and categories of data subjects, and the obligations and rights of the controller (i.e., the business).

It is essential that the processor appointed by the business complies with the GDPR.

**8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?**

The processor must be appointed under a binding agreement in writing. The contractual terms must stipulate that the processor: (i) only acts on the documented instructions of the controller; (ii) imposes confidentiality obligations on all employees; (iii) ensures the security of personal data that it processes; (iv) abides by the rules of regarding the appointment of sub-processors; (v) implements measures to assist the controller with guaranteeing the rights of data subjects; (vi) assists the controller in obtaining approval from the relevant data protection authority; (vii) either returns or destroys the personal data at the end of the relationship (except as required by EU or Member State law); and (viii) provides the controller with all information necessary to demonstrate compliance with the GDPR.

## 9 Marketing

**9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).**

According to the Danish Marketing Practices Act, it is required to obtain a prior opt-in consent from the recipient. There are some modifications for customers of the trader.

**9.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?**

The restrictions are applicable to both business-to-consumer marketing and business-to-business marketing.

**9.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).**

The national opt-out register "*Robinsonlisten*" must be checked in advance before marketing by telephone and post.

Marketing by telephone is legal without consent, when the sole purpose is to sell:

- Books.
- Subscriptions to newspapers and magazines.
- Insurance.
- Rescue services and healthcare subscriptions.

Marketing by telephone is legal where it is business-to-business.

**9.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?**

Yes, European and other international traders must comply with the Danish Marketing Practices Act when sending direct marketing to Danish consumers.

**9.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?**

The supervision authority of the Marketing Practices Act is the Danish Consumer Ombudsman.

The Danish Consumer Ombudsman is very active in the enforcement of breaches of marketing restrictions.

### 9.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

Yes, it is lawful to purchase such lists. However, the receiving party must comply with the Marketing Practices Act. The disclosing party shall comply with Section 13 of the DP Act, which states that an enterprise may not disclose data concerning a consumer to another enterprise for the purpose of direct marketing or use such data on behalf of another enterprise for such marketing purpose unless the consumer has given explicit consent. Consent shall be obtained in accordance with the rules laid down in Section 10 of the Marketing Practices Act.

On certain conditions pursuant to Section 13 of the DP Act, disclosure of general data on customers which form the basis for classification into customer categories may take place without consent. It is a condition that the information can be processed according to Article 6 (1)(f) of the GDPR. It is required that the data controller, prior to disclosure, controls whether the data subjects have opted out of marketing via the opt-out list/ *Robinsonlisten*.

Data controllers who sell lists of groups of persons for direct marketing purposes or who print addresses or distribute messages to such groups on behalf of a third party may only process:

(i) data concerning name, address, position, occupation, email address, telephone and fax number;
(ii) data contained in trade registers which according to law, or provisions laid down by law, are intended for public information; and
(iii) other data if the data subject has given explicit consent. Consent according to Section 13 must be obtained in accordance with Section 10 of the Danish Marketing Practices Act.

### 9.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

When calculating a fine for unlawful direct marketing (spam), the following calculation model applies:

Up to 100 spam mails/SMS will trigger a fine of DKK 10,000. For over 100 spam mail/SMS, an additional fine of DKK 100 for each mail will be given. Thus, the penalty for 60 spam mails/SMS will be DKK 10,000, and for 140 spam mails/SMS the fine will be DKK 14,000.

However, the starting point could derogate in the upward and downward direction if there are aggravating or mitigating circumstances in the specific case.

To our knowledge, the maximum penalty for sending unlawful direct marketing is DKK 800,000 (approx. EUR 107,100).

## 10 Cookies

### 10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

In November 2009, the European Commission adopted Directive 2009/136/EC ("**2009 Directive**"), which amended Directive 2002/58/EC, also known as the e-Privacy Directive. This amendment has been implemented into Danish law by way of Executive Order no. 1148 of 9 December 2011 (the "**Cookie Order**").

The Cookie Order implements Article 5 of the ePrivacy Directive. Pursuant to Article 5 of the EU ePrivacy Directive, the storage of cookies (or other data) on an end user's device requires prior consent (the applicable standard of consent is derived from the GDPR).

On 1 October 2019 the European Court of Justice delivered its judgment in C673/17 (*Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV vs Planet49 GmbH*). The judgment concerns a German company, Planet49, which held an online competition. Participation in the competition was conditioned upon the user giving the company their name and address while simultaneously consenting to receiving marketing from several companies. The user had to check a box concerning consent to participating in the competition. Participation in the competition was, however, not conditioned upon the user giving consent to cookies. Despite this, there was a pre-checked box concerning consent to tracking cookies. As such, the user had to actively uncheck the box if they did not wish to consent.

The judgment addresses two questions: (1) the validity of consent to cookies obtained by using a pre-checked box; and (2) what information companies must give users in relation to the use of cookies.

With the judgment, the European Court of Justice establishes that consent obtained by using a pre-checked box is not valid since an active action from the user is required.

Cookies can only be used if the user has given consent and has been informed about, *inter alia*, the purpose of the processing. This applies regardless of whether personal data is being processed or not. Consent must, to be valid, constitute an active action from the user. This means that consent is invalid if it was obtained by using a pre-checked box or by inactivity.

The European Court of Justice also establishes that a cookie policy must contain information about the duration of the functioning of the cookies and information about whether third parties are in a position to gain access to the cookies or not.

After this judgment, the Danish legal guideline on the Cookie Order was updated on 10 December 2019 and implemented the ruling. Three requirements must be met before consent is valid: (1) the consent must be given before cookies are stored; (2) the consent must be active; and (3) the consent must be informed.

If cookies involve the processing of Personal Data, the Cookie Order as well as the GDPR and the DP Act must be complied with. The DPA has issued a guideline on cookies in February 2020 where it stated that: (1) the consent must be active; (2) the purpose(s) of the processing must be transparent; (3) it must be easy for the visitor of the website to give consent to some purposes and not give consent to others; (4) it must be easy to refuse to give consent; and (5) the owner of the website must be able to document what a visitor has consented to and how the consent was obtained. Furthermore, the DPA and the Danish Business Authority also issued a "Quick guide" in February 2021 regarding the use of cookies.

The Danish Business Authority is the supervisory authority regarding the regulation on the use of cookies. The DPA is also a relevant authority if the use of cookies involves the processing of Personal Data (which is often the case); *cf.* question 10.3.

The EU Commission intends to pass a new ePrivacy Regulation that will replace the respective national legislation in the EU Member States.

**10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?**

There are essentially four different types of cookies:
(1) technically necessary;
(2) functional;
(3) statistical; and
(4) marketing cookies.

Technical cookies (1) which are necessary to perform a service explicitly requested by the user are not regulated by the Cookie Order. Consent to technically necessary cookies is not required, as these help the website to function. Such cookies make a website functional by enabling basic features such as page navigation and access to secure areas of the website. Specifically, these cookies can be divided into two categories: (a) cookies necessary for data transmission so that the website does not break; and (b) cookies that must be there to fulfil the purpose of the website, such as an electronic shopping cart on a webshop and booking systems. Technical cookies also include cookies that ensure that a username and password must only be entered once if requested by the user.

Functional cookies (2) allow you to store information that changes the way the website looks or behaves; for example, a preferred language or region.

Statistical cookies (3) help the website owner understand how visitors interact with the website by collecting and reporting information.

Marketing cookies (4) are used to track visitors across websites and the intention is to serve advertisements that are relevant and engaged to the individual user and are therefore valuable to publishers and third-party advertisers.

**10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?**

Yes, the DPA has expressed serious criticism of processing personal data in connection with the display of banner advertisements on the website of a public authority (a weather report service) without consent (11 February 2020).

Based on the decision from 11 February, the DPA has examined other solutions of consent (22 June and 17 December 2020). In both cases, the DPA focused on an 'active consent' that must not be pre-approved.

**10.4 What are the maximum penalties for breaches of applicable cookie restrictions?**

This is not applicable. The level of fines is not capped.

## 11 Restrictions on International Data Transfers

**11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.**

Data transfers to other jurisdictions that are not within the European Economic Area (the "**EEA**") can only take place if the transfer is to an "Adequate Jurisdiction" (as specified by the EU Commission), the business has implemented one of the required safeguards as specified by the GDPR, or one of the derogations specified in the GDPR applies to the relevant transfer. The EDPB Guidelines (2/2018) set out that a "layered approach" should be taken with respect to these transfer mechanisms. If the transfer is not to an Adequate Jurisdiction, the data exporter should first explore the possibility of implementing one of the safeguards provided for in the GDPR before relying on a derogation.

**11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).**

When transferring personal data to a country other than an Adequate Jurisdiction, businesses must ensure that there are appropriate safeguards on the data transfer, as prescribed by the GDPR. The GDPR offers a number of ways to ensure compliance for international data transfers, of which one is consent of the relevant data subject. Other common options are the use of Standard Contractual Clauses or Binding Corporate Rules ("**BCRs**").

Businesses can adopt the Standard Contractual Clauses drafted by the EU Commission – these are available for transfers between controllers, and transfers between a controller (as exporter) and a processor (as importer). International data transfers may also take place on the basis of contracts agreed between the data exporter and data importer provided that they conform to the protections outlined in the GDPR, and they have prior approval by the relevant data protection authority.

International data transfers within a group of businesses can be safeguarded by the implementation of BCRs. The BCRs will always need approval from the relevant data protection authority. Most importantly, the BCRs will need to include a mechanism to ensure they are legally binding and enforced by every member in the group of businesses. Among other things, the BCRs must set out the group structure of the businesses, the proposed data transfers and their purpose, the rights of data subjects, the mechanisms that will be implemented to ensure compliance with the GDPR and the relevant complainant procedures.

**11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.**

It is likely that the international data transfer will require prior approval from the relevant data protection authority unless they have already established a GDPR-compliant mechanism as set out above for such transfers.

In any case, most of the safeguards outlined in the GDPR will need initial approval from the data protection authority, such as the establishment of BCRs.

**11.4 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?**

The EDPB has issued draft Recommendations 01/2020 on supplementary protections to be implemented where appropriate, in respect of transfers made under Standard Contractual Clauses, in light of the *Schrems II* decision. At the time of writing, those draft Recommendations are not yet finalised.

Following the Court of Justice of the EU's decision in *Schrems II*, the DPA has published recommendations from the European Data Protection Board about transferring personal data to third countries. The recommendations are:

- Processing should be based on clear, precise and accessible rules.
- Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated.
- An independent oversight mechanism should exist.
- Effective remedies need to be available to the individual.

Furthermore, the DPA has published answers and guides for standard questions about the case. The DPA has clarified the relevance of the case and its elements, and how you should act as a data subject, a data controller, and a data processor.

**11.5 What guidance (if any) has/have the data protection authority(ies) issued in relation to the European Commission's revised Standard Contractual Clauses?**

The European Commission has issued draft new Standard Contractual Clauses. The EDPB and the European Data Protection Supervisor have issued Joint Opinion 1/2021 in relation to those draft Standard Contractual Clauses.

The DPA has not issued any guidance in relation to the revised Standard Contractual Clauses in addition to the above.

## 12 Whistle-blower Hotlines

**12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?**

Internal whistle-blowing schemes are generally established in pursuance of a concern to implement proper corporate governance principles in the daily functioning of businesses. Whistle-blowing is designed as an additional mechanism for employees to report misconduct internally through a specific channel and supplements a business' regular information and reporting channels, such as employee representatives, line management, quality-control personnel or internal auditors who are employed precisely to report such misconduct.

The WP29 has limited its Opinion 1/2006 on the application of EU data protection rules to internal whistle-blowing schemes to the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime. The scope of corporate whistle-blower hotlines, however, does not need to be limited to any particular issues. In the Opinion, it is recommended that the business responsible for the whistle-blowing scheme should carefully assess whether it might be appropriate to limit the number of persons eligible for reporting alleged misconduct through the whistle-blowing scheme and whether it might be appropriate to limit the number of persons who may be reported through the scheme; in particular, in the light of the seriousness of the alleged offences reported.

According to the former Danish Act on Processing of Personal Data, the DPA issued a guideline on the processing of personal data in connection with whistle-blower systems. According to the guideline, a company may process information relating to corporate crime, safety-at-work issues, and violation of rules that may have a serious consequence for employees such as sexual harassment or violence. Additionally, information that it would be mandatory to report under the US Sarbanes-Oxley Act may, in the opinion of the DPA, be legally processed in a whistle-blower system. Special categories of information, such as information pertaining to an employee's criminal records, may be processed. However, sensitive information – *cf.* Article 9 of the GDPR – may not be processed. According to several corporate rules, some entities are obliged to establish whistle-blower schemes. The DPA approves that these types of whistle-blower schemes may be legally processed.

**12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?**

Anonymous reporting is not prohibited under EU data protection law; however, it raises problems as regards the essential requirement that personal data should only be collected fairly. In Opinion 1/2006, the WP29 considered that only identified reports should be advertised in order to satisfy this requirement. Businesses should not encourage or advertise the fact that anonymous reports may be made through a whistle-blower scheme.

An individual who intends to report to a whistle-blowing system should be aware that he/she will not suffer due to his/her action. The whistle-blower, at the time of establishing the first contact with the scheme, should be informed that his/her identity will be kept confidential at all the stages of the process, and in particular will not be disclosed to third parties, such as the incriminated person or to the employee's line management. If, despite this information, the person reporting to the scheme still wants to remain anonymous, the report will be accepted into the scheme. Whistle-blowers should be informed that their identity may need to be disclosed to the relevant people involved in any further investigation or subsequent judicial proceedings instigated as a result of any enquiry conducted by the whistle-blowing scheme.

## 13 CCTV

**13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?**

A data protection impact assessment ("**DPIA**") must be undertaken with assistance from the Data Protection Officer when there is systematic monitoring of a publicly accessible area on a large scale. If the DPIA suggests that the processing would result in a high risk to the rights and freedoms of individuals prior to any action being taken by the controller, the controller must consult the data protection authority.

During the course of a consultation, the controller must provide information on the responsibilities of the controller and/or processors involved, the purpose of the intended processing, a copy of the DPIA, the safeguards provided by the GDPR to protect the rights and freedoms of data subjects and, where applicable, the contact details of the Data Protection Officer.

If the data protection authority is of the opinion that the CCTV monitoring would infringe the GDPR, it has to provide written advice to the controller within eight weeks of the request of a consultation and can use any of its wider investigative, advisory and corrective powers outlined in the GDPR.

Danish Act no. 1190 of 11 October 2007 regarding CCTV is supervised by the Danish National Police. The Act regulates private controllers' use of CCTV. The Act has specific provisions regarding the transfer of personal data from CCTV.

**13.2 Are there limits on the purposes for which CCTV data may be used?**

Yes, CCTV may only be used for the purpose of preventing crime and for security purposes.

## 14 Employee Monitoring

**14.1 What types of employee monitoring are permitted (if any), and in what circumstances?**

Employees can be monitored when the following conditions are met:

- The monitoring is justified for operational reasons and according to a fair purpose.
- The monitoring is not offensive to the employees.
- The monitoring does not cause losses or significant disadvantages.
- The monitoring is proportional according to its purpose.
- The employee shall be given six weeks' notice. If the purpose or operational reasons make it necessary, monitoring can be initiated without notice.

Examples of employee monitoring include email and internet access, CCTV, time recorders, etc.

**14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.**

Notice is required, and the notice is typically given in connection with the employment agreement.

**14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?**

If the company has a work council, such work council should be notified; alternatively, the union representative should be notified if not the council.

It is recommended that an actual local agreement be concluded on the control measures and on any consequences of an infringement.

## 15 Data Security and Data Breach

**15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?**

Yes. Personal data must be processed in a way which ensures security and safeguards against unauthorised or unlawful processing, accidental loss, destruction and damage of the data.

Both controllers and processors must ensure they have appropriate technical and organisational measures to meet the requirements of the GDPR. Depending on the security risk, this may include: the encryption of personal data; the ability to ensure the ongoing confidentiality, integrity and resilience of processing systems; an ability to restore access to data following a technical or physical incident; and a process for regularly testing and evaluating the technical and organisational measures for ensuring the security of processing.

**15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

The controller is responsible for reporting a personal data breach without undue delay (and in any case within 72 hours of first becoming aware of the breach) to the relevant data protection authority, unless the breach is unlikely to result in a risk to the rights and freedoms of the data subject(s). A processor must notify any data breach to the controller without undue delay.

The notification must include the nature of the personal data breach, including the categories and number of data subjects concerned, the name and contact details of the Data Protection Officer or relevant point of contact, the likely consequences of the breach, and the measures taken to address the breach, including attempts to mitigate possible adverse effects.

**15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

Controllers have a legal requirement to communicate the breach to the data subject, without undue delay, if the breach is likely to result in a high risk to the rights and freedoms of the data subject.

The notification must include the name and contact details of the Data Protection Officer (or point of contact), the likely consequences of the breach, and any measures taken to remedy or mitigate the breach.

The controller may be exempt from notifying the data subject if the risk of harm is remote (e.g., because the affected data is encrypted), the controller has taken measures to minimise the risk of harm (e.g., suspending affected accounts) or the notification requires a disproportionate effort (e.g., a public notice of the breach).

**15.4 What are the maximum penalties for data security breaches?**

The maximum penalty is the higher of EUR 20 million or 4% of worldwide turnover.

## 16 Enforcement and Sanctions

**16.1 Describe the enforcement powers of the data protection authority(ies).**

(a) **Investigative Powers**: The DPA has wide powers to order the controller and the processor to provide any information it requires for the performance of its tasks, to conduct investigations in the form of data protection audits, to carry out a review on certificates issued pursuant to the GDPR, to notify the controller or processor of alleged infringement of the GDPR, to access all personal data and all information necessary for the performance of controllers' or processors' tasks and access to the premises of the data including any data processing equipment.

(b) **Corrective Powers**: The DPA has a wide range of powers including the ability to issue warnings or reprimands for non-compliance, to order the controller to disclose a personal data breach to the data subject, to impose a permanent or temporary ban on processing, to withdraw a certification and to recommend a fine (as below).

(c) **Authorisation and Advisory Powers**: The DPA has a wide range of powers to advise the controller, accredit certification bodies and to authorise certificates, contractual clauses, administrative arrangements and binding corporate rules as outlined in the GDPR.
The opinion of the DPA shall be obtained from legislative proposals, executive orders, circulars or similar general regulations that affect the protection of privacy in connection with the processing of personal data.

(d) **Imposition of administrative fines for infringements of specified GDPR provisions**: The legal system of Denmark does not allow for administrative fines as set out in the GDPR. However, the GDPR states that the competent national courts should take into account the recommendation by the supervisory authority initiating the fine. In any event, the fines imposed should be effective, proportionate and dissuasive.

(e) The GDPR provides for administrative fines which can be EUR 20 million or up to 4% of the business' worldwide annual turnover of the proceeding financial year, and the Danish courts are bound by this.

(f) **Non-compliance with a data protection authority**: As mentioned above, the Danish legal system does not allow for administrative fines as set out in the GDPR. Therefore, the DPA may not impose fines for non-compliance, but could instead recommend a fine and file a police report after which the prosecution must conduct the case and the final fine is imposed by competent national courts as a criminal penalty. Also, the DPA may file a civil case with the Danish courts.

### 16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The GDPR entitles the relevant data protection authority to impose a temporary or definitive limitation including a ban on processing.

The DP Act may in exceptional cases prohibit, restrict, or suspend the transfer to a third country or an international organisation of information according to Article 9(1) of the GDPR in cases where a decision has not been adopted concerning the adequacy of the level of protection under Article 45 of the GDPR.

### 16.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

As mentioned in question 16.1, the DPA is not authorised to give administrative fines but can instead recommend a fine and file a police report, after which the prosecution must conduct the case, and competent national courts impose the final fine.

At this time (March 2021), the DPA has filed eight police reports, four of which have been to companies and four of which have been to public authorities. One of the cases has been in court.

The first case concerns a company where the DPA recommended a fine of DKK 1.5 million (approximately EUR 200,750) in June 2019. The violation regards the failure of deletion, and in this case, it was personal data regarding 385,000 customers. The company had been processing personal data for a longer period than necessary for the purposes for which they were processed. To ensure that the personal data were not kept longer than necessary, the company should have complied with its time limits.

In February 2021, the Court of First Instance sentenced a fine of DKK 100,000. The decision was based on that it was a matter of negligence, that the company had strived to be compliant, and the fine was calculated based on the individual company and not the turnover for the total group of companies. Further, the fine was based on the company's first-time infringement; the personal data was not sensitive; the data was placed in an old and phased out system and endangered no data subjects. The verdict has been appealed.

Two other cases concern lack of deletion of personal data and therefore unlawful processing of personal data in two companies, and the DPA have recommended fines of DKK 1.2 million (approximately EUR 161,500) and DKK 1.1 million (approximately EUR 148,000).

Four other cases concern the security of processing, and the DPA has recommended fines of DKK 50,000 (approximately EUR 6,700) to two public authorities, DKK 100,000 (approximately EUR 13,400) to another public authority and a fine of DKK 150,000 (approximately EUR 20,100) to a company.

Further, the DPA has recommended a fine of DKK 50,000 (approximately EUR 6,700) to one public authority concerning the notification of a personal data breach.

The DPA can issue reprimands where processing operations have infringed provisions of the GDPR or order a company to bring processing operations into compliance with the GDPR.

The DPA has been active in the enforcement within its authorisation, and there are at this point many decisions from the DPA where the DPA either has issued reprimands or ordered a company to bring processing operations into compliance with the rules.

In general, the decisions are about:

- The principles of the processing of personal data.
- The basis of the processing. The DPA has, for example, prohibited a company from recording telephone conversations without obtaining a consent to do so, as they decided that the processing could not be done within the purposes of the legitimate interests pursued by the company.
- The rights of the data subject. For example, the DPA has issued severe reprimands where a company could not erase a data subject, and it was not sufficient that the inaccurate personal data were rectified.
- Security of processing. The DPA has issued a reprimand to a company over the use of the encryption form TLS (encryption in the transport layer) without further control. This was not a sufficient security measure and, therefore, when sending confidential and sensitive information, forced TLS to be used.
- Notification of a personal data breach to the supervisory authority. For example, the DPA has ordered a company to communicate the personal data breach to the data subject.
- The lack of designation of a Data Protection Officer.

### 16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

The "one-stop shop" mechanism of the GDPR regulates where the Danish DPA has jurisdiction in another Member State.

In October 2019, the DPA ordered an international company to bring processing operations into compliance with the

provisions of the GDPR regarding the deletion of personal data about a British data subject. The DPA issued reprimands to this company regarding the processing of personal data that did not comply with the GDPR. The company had a practice where it requested passport identification from data subjects trying to exercise their rights under the GDPR without making a specific assessment on whether there is reasonable doubt as to the identity of the data subject.

This is the first case which the Danish DPA has decided as the lead supervisory authority under the "one-stop-shop mechanism" in connection with cross-border processing of personal data.

## 17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

### 17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Foreign law enforcement authorities requesting information from Danish entities, etc., must send a letter rogatory to the Danish law enforcement authorities regarding the information needed. In this case, the Danish law enforcement authorities may try to get a court order or to obtain acknowledgment of a foreign court order.

A Danish data controller is only permitted to disclose personal data according to the regulation on processing of personal data (primarily, the GDPR or the DP Act).

### 17.2 What guidance has/have the data protection authority(ies) issued?

There is no specific guidance on the subject.

## 18 Trends and Developments

### 18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

**IT-University of Copenhagen – File number: 2020-432-0034**
The Danish DPA investigated the processing of personal data of the IT-University of Copenhagen. During COVID-19 the students had to do the examinations from home. The DPA investigated the IT programmes, which were used to monitor the students. In this connection, the DPA concluded that the university complied with the principles relating to the processing of personal data, including the fact that the university had chosen the least-intrusive way to achieve the purpose.

**The medical guard in the region of Southern Denmark – File number: 2019-32-0988**
The Danish DPA investigated the processing of personal data of the medical guard in the region of Southern Denmark. The patients' phone calls were stored more than five years since the medical guard considered the phone calls to be a part of a patient's medical record, which may be stored for up to 10 years. However, the Danish DPA did not consider the phone calls as a part of the medical records, nor why such phone calls can only be stored for five years (the end of a patient's right to appeal).

We have noted the following trends from the DPA:

- The DPA has stated that the first police report was filed because of the considerable amount of personal data which happened to be stored without a valid purpose.
- The DPA has had an increased focus on the security of processing of companies and public authorities, and whether they have implemented appropriate technical and organisational measures to ensure a level of security appropriate to the risk.
- As described above, only one of eight cases where the DPA has filed a police report has been in court. Regardless of whether the DPA recommended a fine of DKK 1.5 million (approximately EUR 200,750) and the verdict has been appealed, it is worth noticing the Court of First Instance sentenced a fine of DKK 100,000. The size of the fine was based on the fact that i) it was a matter of negligence, ii) the company had strived to be compliant, iii) the fine was calculated based on the individual company and not the turnover for the total group of companies, iv) the fine was based on the company's first-time infringement, v) the personal data was not sensitive, and vi) the data was placed in an old and phased out system and endangered no data subjects.

### 18.2 What "hot topics" are currently a focus for the data protection regulator?

The DPA has published its focus areas for 2021. These are:

- Credit reference agencies, registers of warning and barring-lists.
- Recovery agencies obligation to provide information and erasure.
- Financial institutions procedure for requests for access.
- Television surveillance.
- Authorities transfer of identity numbers to citizens.
- Research
- The processing of personal data for visitors on websites (cookies)
- Security of personal data, including personal data breach.
- Control of data processors.
- Transfer of personal data to third countries.
- Processing of personal data in pan-European information systems.
- The PNR Act.
- The Enforcement Act.

**Heidi Højmark Helveg** specialises in marketing law, privacy law/GDPR and intellectual property law.
In recent years, she has focused on providing advice relating to marketing law, personal data law and media law, and over the years, she has also gained solid expertise in intellectual property law (especially trademark law and copyright law). She represents Danish and international companies, organisations and public authorities. Her experience in marketing law was enhanced when she was appointed as a member of the Danish Government's Marketing Law Commission at the end of 2014, upon recommendation by the Association of Danish Law Firms and the Danish Bar and Law Society.

**CO:PLAY Advokatpartnerselskab**
Strandvejen 58, 1.
2900 Hellerup
Copenhagen
Denmark

Tel: +45 30 74 29 00
Email: hhh@coplay.law
URL: www.coplay.law

**Niels Dahl-Nielsen** specialises in data protection/GDPR, IT law and cybersecurity. He has mainly represented companies in the IT industry within various segments, particularly software development and software consultancy companies, and one leading global cloud service provider regarding highly complex personal data protection law matters. Niels holds experience in representing Danish and international corporations on all issues related to data protection and public bodies. Furthermore, Niels is a Danish Data Protection Association member and holds seminars for lawyers and data protection officers regarding the General Data Protection Regulation.

**CO:PLAY Advokatpartnerselskab**
Strandvejen 58, 1.
2900 Hellerup
Copenhagen
Denmark

Tel: +45 40 30 97 49
Email: ndn@coplay.law
URL: www.coplay.law

CO:PLAY is a modern and highly specialised law firm focusing on technology, media and entertainment. Our team of advisors provide expert advice based on our clients' business and their use of technology. CO:PLAY is a commercial law firm with corporate, commercial, intellectual property, litigation, IT, telecoms, data protection and marketing practices. Leading international legal ranking institutes acknowledge several of our lawyers. CO:PLAY offers in-depth business insight about tech and IT and knowledge about its customers' daily business. We believe that legal services should be available for small start-ups as well as established companies. For this reason, we incorporate digital technology in delivering their legal services and lower the perceived threshold that many companies have when seeking legal consulting. CO:PLAY has its office in Copenhagen, Denmark.

**www.coplay.law**

# France


Boriana Guimberteau


Clémence Louvet

Foucaud Tchekhoff Pochet et Associés (FTPA)

## 1 Relevant Legislation and Competent Authorities

### 1.1 What is the principal data protection legislation?

Since 25 May 2018, the principal data protection legislation in the EU has been Regulation (EU) 2016/679 (the "General Data Protection Regulation" or "GDPR"). The GDPR repealed Directive 95/46/EC (the "Data Protection Directive") and has led to increased (though not total) harmonisation of data protection law across the EU Member States.

The domestic data protection regulation includes the French Data Protection Act 78-17 of 6 January 1978 modified by Law 2018-493 of 20 June 2018 ("French Data Protection Act") and Decree 2019-536 of 20 June 2018 implementing the provisions of the General Data Protection Regulation (GDPR). Law 2018-493 has been updated by Ordinance n°2018-1125 dated 12 December 2018, applicable since 1 June 2019.

### 1.2 Is there any other general legislation that impacts data protection?

In addition to the GDPR, the European Union has adopted the (EU) Directive of 27 April 2016, the so-called "Police Justice Directive" on the processing of personal data in criminal matters. These two acts constitute the "European package" regulating data protection.

The French post and electronic communications code includes article L. 34-5, which requires the prior consent of the consumers before sending fax and emails in accordance with the requirements of Directive 2002/58/EC (as amended by Directive 2009/136/EC) ("ePrivacy Directive").

On 10 February 2021, the Council of the European Union announced the agreement of the Member States on a proposal for an ePrivacy regulation that would harmonise the applicable rules across the EU and update Directive 2002/58/EC on privacy and electronic communications to consider new market actors and technological and recent commercial developments.

The ePrivacy Regulation is still a draft at this stage and it is unclear when it will be finalised, but the text is about to be debated in the European Parliament and in the European Council, which will specify the details of the text later.

The EU Directive on the Security of Network and Information Systems ("NIS") implemented in France on 6 February 2019 by French Law n°2018-133, also impacts data protection by providing legal measures to boost the overall level of cybersecurity.

### 1.3 Is there any sector-specific legislation that impacts data protection?

The French Supervisory Authority, i.e. the *Commission Nationale de l'Informatique et des Libertés* ("CNIL"), may issue guidelines and recommendations on data protection-related matters.

In addition, Article 154 of Law n° 2019-1479 of 28 December 2019 on finance for 2020 gave the tax and customs administrations, on an experimental basis and for a period of three years, the right to use personal data made public by taxpayers on the internet. The conditions of application of this Law were specified by the Decree 2021-148 of 11 February 2021.

### 1.4 What authority(ies) are responsible for data protection?

The CNIL is the authority responsible for data protection.

## 2 Definitions

### 2.1 Please provide the key definitions used in the relevant legislation:

- "**Personal Data**"
  Personal Data means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- "**Processing**"
  Processing means any operation or set of operations that is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- "**Controller**"
  Controller means the natural or legal person, public authority, agency or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data.
- "**Processor**"
  Processor means a natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller.

- "**Data Subject**"
  Data Subject means an individual who is the subject of the relevant personal data.
- "**Sensitive Personal Data**"
  Sensitive Personal Data are personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health or sex life and sexual orientation, genetic data or biometric data.
- "**Data Breach**"
  Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

## 3 Territorial Scope

### 3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The GDPR applies to businesses that are established in any EU Member State, and that process personal data (either as a controller or processor, and regardless of whether or not the processing takes place in the EU) in the context of that establishment.

A business that is not established in a Member State but is subject to the laws of a Member State by virtue of public international law is also subject to the GDPR.

The GDPR applies to businesses outside the EU if they (either as controller or processor) process the personal data of EU residents in relation to: (i) the offering of goods or services (whether or not in return for payment) to EU residents; or (ii) the monitoring of the behaviour of EU residents (to the extent that such behaviour takes place in the EU).

Further, the GDPR applies to businesses established outside the EU if they monitor the behaviour of EU residents (to the extent such behaviour takes place in the EU).

## 4 Key Principles

### 4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  Personal data must be processed lawfully, fairly and in a transparent manner. Controllers must provide certain minimum information to data subjects regarding the collection and further processing of their personal data. Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
- **Lawful basis for processing**
  Processing of personal data is lawful only if, and to the extent that, it is permitted under EU data protection law. Article 6 of the GDPR provides an exhaustive list of legal bases on which personal data may be processed, of which the following are the most relevant for businesses: (i) prior, freely given, specific, informed and unambiguous consent of the data subject; (ii) contractual necessity (i.e., the processing is necessary for the performance of a contract to which the data subject is a party, or for the purposes of pre-contractual measures taken at the data subject's request); (iii) compliance with legal obligations (i.e., the controller has a legal obligation, under the laws of the EU or an EU Member State, to perform the relevant processing); or (iv) legitimate interests (i.e., the processing is necessary for the purposes of legitimate interests pursued by the controller, except where the controller's interests are overridden by the interests, fundamental rights or freedoms of the affected data subjects).
  Businesses require stronger grounds to process sensitive personal data. The processing of sensitive personal data is only permitted under certain conditions, of which the most relevant for businesses are: (i) explicit consent of the affected data subject; (ii) the processing is necessary in the context of employment law; or (iii) the processing is necessary for the establishment, exercise or defence of legal claims.
- **Purpose limitation**
  Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes. If a controller wishes to use the relevant personal data in a manner that is incompatible with the purposes for which they were initially collected, it must: (i) inform the data subject of such new processing; and (ii) be able to rely on a lawful basis as set out above.
- **Data minimisation**
  Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which the data is processed. A business should only process personal data that it actually needs to process in order to achieve its processing purposes.
- **Accuracy**
  Personal data must be accurate and, where necessary, kept up to date. A business must take every reasonable step to ensure that personal data that are inaccurate are either erased or rectified without delay.
- **Retention**
  Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.
- **Data security**
  Personal data must be processed in a manner that ensures its appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- **Accountability**
  The controller is responsible for, and must be able to demonstrate, compliance with the data protection principles set out above.

## 5 Individual Rights

### 5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**
  A data subject has the right to obtain from a controller the following information in respect of the data subject's personal data: (i) confirmation of whether, and where, the controller is processing the data subject's personal data; (ii) information about the purposes of the processing; (iii) information about the categories of data being processed; (iv) information about the categories of recipients with whom the data may be shared; (v) information about the period for which the data will be stored (or the criteria used to determine that period); (vi) information about

the existence of the rights to erasure, to rectification, to restriction of processing and to object to processing; (vii) information about the existence of the right to complain to the relevant data protection authority; (viii) where the data were not collected from the data subject, information as to the source of the data; and (ix) information about the existence of, and an explanation of the logic involved in, any automated processing that has a significant effect on the data subject.

Additionally, the data subject may request a copy of the personal data being processed.

- **Right to rectification of errors**
  Controllers must ensure that inaccurate or incomplete data are erased or rectified. Data subjects have the right to rectification of inaccurate personal data.
- **Right to deletion/right to be forgotten**
  Data subjects have the right to erasure of their personal data (the "right to be forgotten") if: (i) the data are no longer needed for their original purpose (and no new lawful purpose exists); (ii) the lawful basis for the processing is the data subject's consent, the data subject withdraws that consent, and no other lawful ground exists; (iii) the data subject exercises the right to object, and the controller has no overriding grounds for continuing the processing; (iv) the data have been processed unlawfully; or (v) erasure is necessary for compliance with EU law or national data protection law.
- **Right to object to processing**
  Data subjects have the right to object, on grounds relating to their particular situation, to the processing of personal data where the basis for that processing is either public interest or legitimate interest of the controller. The controller must cease such processing unless it demonstrates compelling legitimate grounds for the processing which overrides the interests, rights and freedoms of the relevant data subject or requires the data in order to establish, exercise or defend legal rights.
- **Right to restrict processing**
  Data subjects have the right to restrict the processing of personal data, which means that the data may only be held by the controller, and may only be used for limited purposes if: (i) the accuracy of the data is contested (and only for as long as it takes to verify that accuracy); (ii) the processing is unlawful and the data subject requests restriction (as opposed to exercising the right to erasure); (iii) the controller no longer needs the data for their original purpose, but the data are still required by the controller to establish, exercise or defend legal rights; or (iv) verification of overriding grounds is pending, in the context of an erasure request.
- **Right to data portability**
  Data subjects have a right to receive a copy of their personal data in a commonly used machine-readable format and transfer their personal data from one controller to another or have the data transmitted directly between controllers.
- **Right to withdraw consent**
  A data subject has the right to withdraw their consent at any time. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject must be informed of the right to withdraw consent. It must be as easy to withdraw consent as to give it.
- **Right to object to marketing**
  Data subjects have the right to object to the processing of personal data for the purpose of direct marketing, including profiling.
- **Right to complain to the relevant data protection authority(ies)**
  Data subjects have the right to lodge complaints concerning the processing of their personal data with CNIL if the data subjects live in France or the alleged infringement occurred in France.
- **Right to basic information**
  Data subjects have the right to be provided with information on the identity of the controller, the reasons for processing their personal data and other relevant information necessary to ensure the fair and transparent processing of personal data.

## 6 Registration Formalities and Prior Approval

**6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?**

There is no obligation to notify CNIL since the GDPR came into force on 25 May 2018. However, there is an exception that relates to the processing of health data presenting a public interest pursuant to Article 66 of the French Data Protection Act, e.g. processing related to the safety of drugs and patient care. An authorisation from CNIL or CNIL's opinion may be necessary in this event.

The GDPR requires businesses to maintain a record of processing activities in accordance with articles 30 and 31 of the GDPR. This record must describe the processing carried out by businesses. This record does not have to be registered with CNIL.

CNIL recommends maintaining two records if the organisation acts both as a processor and as a data controller.

Also, a data protection impact assessment ("DPIA") is required for processing that would most likely result in a high risk to the rights and freedoms of natural persons, in accordance with article 35 of the GDPR. It concerns, notably, processing using new technologies.

**6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?**

This is not applicable.

**6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?**

This is not applicable.

**6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?**

This is not applicable.

**6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?**

This is not applicable.

**6.6 What are the sanctions for failure to register/notify where required?**

This is not applicable.

**6.7 What is the fee per registration/notification (if applicable)?**

This is not applicable.

**6.8 How frequently must registrations/notifications be renewed (if applicable)?**

This is not applicable.

**6.9 Is any prior approval required from the data protection regulator?**

This is not applicable.

**6.10 Can the registration/notification be completed online?**

This is not applicable.

**6.11 Is there a publicly available list of completed registrations/notifications?**

This is not applicable.

**6.12 How long does a typical registration/notification process take?**

This is not applicable.

## 7 Appointment of a Data Protection Officer

**7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.**

According to Articles 37 *et seq.* of the GDPR, the appointment of a Data Protection Officer ("DPO") for controllers or processors is mandatory in some circumstances, including where there is: (i) large-scale regular and systematic monitoring of individuals; or (ii) large-scale processing of sensitive personal data.

The appointment of a DPO is also mandatory when the processing of Personal Data is carried out by a public authority or public body, with the exception of judicial courts.

Where a business designates a DPO voluntarily, the requirements of the GDPR apply as if the appointment was mandatory.

**7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?**

In the circumstances where appointment of a DPO is mandatory, failure to comply may result in the wide range of penalties available under the GDPR.

**7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?**

The appointed DPO should not be dismissed or penalised for performing his/her tasks and should report directly to the highest management level of the controller or processor.

It is the controller or processor that is responsible and must demonstrate that processing complies with the Regulation.

**7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?**

A single DPO is permitted by a group of undertakings provided that the DPO is easily accessible from each entity.

**7.5 Please describe any specific qualifications for the Data Protection Officer required by law.**

The DPO should be appointed on the basis of professional qualities and should have an expert knowledge of data protection law and practices. While this is not strictly defined, it is clear that the level of expertise required will depend on the circumstances. For example, the involvement of large volumes of sensitive personal data will require a higher level of knowledge.

**7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?**

A DPO should be involved in all issues that relate to the protection of personal data. The GDPR outlines the minimum tasks required by the DPO, which include: (i) informing the controller, processor and their relevant employees who process data of their obligations under the GDPR; (ii) monitoring compliance with the GDPR, national data protection legislation and internal policies in relation to the processing of personal data including internal audits; (iii) advising on data protection impact assessments and the training of staff; and (iv) co-operating with the data protection authority and acting as the authority's primary contact point for issues related to data processing.

**7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?**

Yes, the controller or processor must notify CNIL of the contact details of the designated DPO. The registration form is available online via: https://designations.cnil.fr/dpo/designation/organisme.designant.delegue.action.

**7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?**

The DPO does not necessarily need to be named in the

public-facing privacy notice. However, the contact details of the DPO must be notified to the data subject when personal data relating to that data subject is collected. As a matter of good practice, Article 29 Working Party (the "WP29") (now the European Data Protection Board (the "EDPB")) recommended in its 2017 guidance on Data Protection Officers that both the data protection authority and employees should be notified of the name and contact details of the DPO.

## 8 Appointment of Processors

**8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?**

Yes. The business that appoints a processor to process personal data on its behalf, is required to enter into an agreement with the processor which sets out the subject matter for processing, the duration of processing, the nature and purpose of processing, the types of personal data and categories of data subjects and the obligations and rights of the controller (i.e., the business).

It is essential that the processor appointed by the business complies with the GDPR.

**8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?**

The processor must be appointed under a binding agreement in writing. The contractual terms must stipulate that the processor: (i) only acts on the documented instructions of the controller; (ii) imposes confidentiality obligations on all employees; (iii) ensures the security of personal data that it processes; (iv) abides by the rules regarding the appointment of sub-processors; (v) implements measures to assist the controller with guaranteeing the rights of data subjects; (vi) assists the controller in obtaining approval from the relevant data protection authority; (vii) either returns or destroys the personal data at the end of the relationship (except as required by EU or Member State law); and (viii) provides the controller with all information necessary to demonstrate compliance with the GDPR.

## 9 Marketing

**9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).**

Prior authorisation shall be expressly obtained before sending direct marketing of consumers (article L. 34-5 of the French post and electronic communications code). Prior consent is not required for consumers who have already purchased similar products or services, or if the canvassing is not of a commercial nature. In both cases, data subjects must be informed that their email address will be used for canvassing purposes and have right to object, at any time, to receiving marketing emails (e.g. through an unsubscribe link at the end of the message).

Any consumer receiving telephone or SMS spam may transfer them to "33 700" and block the telephone or SMS spam.

**9.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?**

In a business-to-business context, the natural person: (i) must be informed, at the time of collecting his/her email address, that it will be used for canvassing purposes; and (ii) has the right to object at any time to receiving marketing emails.

**9.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).**

In order to implement the principles of Article L. 34-5 of the French post and electronic communications code and French Data Protection Act 78-17 of 6 January 1978, any consumer may register him/herself in a list of opposition to outbound calls, called bloctel (http://www.bloctel.gouv.fr/). The registration on that list lasts for a period of three years and may be renewed every three years. Companies are forbidden to call consumers registered on this list, unless (i) the consumer is a previous and/or current client of the company, (ii) the company is selling subscriptions to newspapers or magazines, or (iii) the company is a polling institute or a non-profit organisation for a non-commercial purpose.

In the event of previous relationships between the company and the consumer:

(i) The company shall nevertheless inform the consumer that he/she declare his/her opposition to future marketing calls.

(ii) The company is no longer entitled to call the consumer after the end of the service concerned (e.g., the purchased good was delivered) if the consumer is registered on the Bloctel list.

If the consumer has communicated his/her phone number to be called back, the company is only entitled to call this number within three months of the communication of the phone number.

**9.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?**

Yes, if the marketing is related to the offering of goods or services to a French consumer.

**9.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?**

The consumer may file a complaint online before the Bloctel agency against companies calling him/her in breach of his/her registration on that list, or before the CNIL.

**9.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?**

Yes, as long as the consumers included in the list consented to the transfer of their personal data to a third party and provided that the transfer is itself GDPR-compliant.

**9.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?**

The maximum criminal penalties are five year's imprisonment and a fine of 300,000 Euros (for individuals) or 1.5 million Euros (if the company is held liable). In addition, a maximum administrative fine of 20 million Euros may be issued by CNIL.

## 10 Cookies

**10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).**

The French Data Protection Act implements article 5 of the ePrivacy Directive. Pursuant to Article 5(3) of the EU ePrivacy Directive (Directive 2002/58/EC), amended in 2009, the storage of cookies (or other data) on an end user's device requires prior consent, unless this storage is necessary for the provision of an online communication service expressly requested by the user or is exclusively for the purpose of enabling or facilitating a communication by electronic means.

The CNIL recalled that such "consent" refers to the definition and conditions set out in Articles 4(11) and 7 of the GDPR. Thus, it must be free, specific, informed and unambiguous, and the user must be able to withdraw it at any time, as easily it was given.

The CNIL has also adopted guidelines applicable to the deposit and reading of trackers in the user's terminal on 17 September 2020. They are supplemented by a recommendation which provides examples of practical ways of collecting consent.

The EU Commission intends to pass a new ePrivacy Regulation that will replace the respective EU Member States' national legislation.

**10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?**

Yes, the applicable restrictions distinguish between different types of cookies. Among cookies requiring prior information and consent for the user, there are:

- cookies linked to personalised advertising; and
- social network cookies, namely those generated by their sharing buttons.

Trackers not subject to consent include:

- trackers that retain the choice expressed by users on the deposit of trackers;
- trackers intended to keep track of the contents of a shopping cart on a merchant site or to invoice the user's purchases;
- trackers allowing load balancing of equipment contributing to a communication service; and
- certain audience measurement trackers.

**10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?**

Yes, the CNIL adopted amending guidelines and a recommendation on the use of cookies and other trackers on 17 September 2020, which came into force on 1 October 2020.

As an example, CNIL took the following enforcement actions:

- on 7 December 2020, CNIL fined Google LLC and Google Ireland Limited a total of 100 million Euros, in particular for having placed advertising cookies on the computers of users of the google.fr browser without prior consent or satisfactory information following investigations online; and
- on 7 December 2020, CNIL fined Amazon Europe Core 35 million Euros for placing advertising cookies on users' computers from the amazon.fr website without prior consent and without satisfactory information following investigations.

**10.4 What are the maximum penalties for breaches of applicable cookie restrictions?**

Violations of cookies provisions are subject to administrative fines of up to 20 million Euros or, in the case of a business, up to 4% of the total worldwide annual turnover in the preceding business year, whichever is higher.

## 11 Restrictions on International Data Transfers

**11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.**

Data transfers to other jurisdictions that are not within the European Economic Area (the "EEA") can only take place if the transfer is to an "Adequate Jurisdiction" (as specified by the EU Commission), if the business has implemented one of the required safeguards as specified by the GDPR, or if one of the derogations specified in the GDPR applies to the relevant transfer. The EDPB Guidelines (2/2018) set out that a "layered approach", should be taken with respect to these transfer mechanisms. If the transfer is not to an Adequate Jurisdiction, the data exporter should first explore the possibility of implementing one of the safeguards provided for in the GDPR before replying on a derogation.

**11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).**

When transferring personal data to a country other than an Adequate Jurisdiction, businesses must ensure that there are appropriate safeguards on the data transfer, as prescribed by the GDPR. The GDPR offers a number of ways to ensure compliance for international data transfers, one of which is consent of the relevant data subject. Other common options are the use of Standard Contractual Clauses or Binding Corporate Rules ("BCRs").

Businesses can adopt the Standard Contractual Clauses drafted by the EU Commission – these are available for transfers between controllers, and transfers between a controller (as exporter) and a processor (as importer). International data transfers may also take place on the basis of contracts agreed between the data exporter and data importer provided that they conform to the protections outlined in the GDPR, and they have prior approval by the relevant data protection authority.

International data transfers within a group of businesses can be safeguards by the implementation of BCRs. The BCRs will always need approval from the relevant data protection authority. Most importantly, the BCRs will need to include a mechanism to ensure they are legally binding and enforced by every member in

the group of businesses. Among other things, the BCRs must set out the group structure of the businesses, the proposed data transfers and their purpose, the rights of data subjects, the mechanisms that will be implemented to ensure compliance with the GDPR and the relevant complainant procedures.

**11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.**

It is likely that the international data transfer will require prior approval from the relevant data protection authority unless they have already established a GDPR-compliant mechanism as set out above for such transfers.

In any case, most of the safeguards outlined in the GDPR will need initial approval from the data protection authority, such as the establishment of BCRs.

**11.4 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?**

On 10 November 2020, the EDPB issued Recommendations 01/2020 on supplementary protections to be implemented where appropriate, in respect of transfers made under Standard Contractual Clauses, in light of the *Schrems II* decision. This recommendation was put out to public consultation until 21 December 2020. (At the time of writing, these draft Recommendations had not yet been finalised.)

**11.5 What guidance (if any) has/have the data protection authority(ies) issued in relation to the European Commission's revised Standard Contractual Clauses?**

The European Commission has issued new Standard Contractual Clauses. The EDPB and the European Data Protection Supervisor have issued Joint Opinion 1/2021 in relation to those draft Standard Contractual Clauses. (At the time of writing, the new Standard Contractual Clauses had not yet been finalised.)

## 12 Whistle-blower Hotlines

**12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?**

Internal whistle-blowing schemes are generally established in pursuance of a concern to implement proper corporate governance principles in the daily functioning of businesses. Whistle-blowing is designed as an additional mechanism for employees to report misconduct internally through a specific channel and supplements a business regular information and reporting channels, such as employee representatives, line management, quality-control personnel or internal auditors who are employed precisely to report such misconduct.

The WP29 has limited its Opinion 1/2006 on the application of EU data protection rules to internal whistle-blowing schemes to the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime. The scope of corporate whistle-blower hotlines, however, does not need to be limited to any particular issues. In the Opinion, it is recommended that the business responsible for the whistle-blowing scheme should carefully assess whether it might be appropriate to limit the number of persons eligible for reporting alleged misconduct through the whistle-blowing scheme and whether it might be appropriate to limit the number of persons who may be reported through the scheme; in particular, in the light of the seriousness of the alleged offences reported.

**12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?**

Anonymous reporting is not prohibited under EU data protection law; however, it raises problems as regards the essential requirement that personal data should only be collected fairly. In Opinion 1/2006, the WP29 considered that only identified reports should be advertised in order to satisfy this requirement. Businesses should not encourage or advertise the fact that anonymous reports may be made through a whistle-blower scheme.

An individual, who intends to report to a whistle-blowing system should be aware that he/she will not suffer due to his/her action. The whistle-blower, at the time of establishing the first contact with the scheme, should be informed that his/her identity will be kept confidential at all the stages of the process, and in particular will not be disclosed to third parties, such as the incriminated person or the employee's line management. If, despite this information, the person reporting to the scheme still wants to remain anonymous, the report will be accepted into the scheme. Whistle-blowers should be informed that their identity may need to be disclosed to the relevant people involved in any further investigation or subsequent judicial proceedings instigated as a result of any enquiry conducted by the whistle-blowing scheme.

## 13 CCTV

**13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?**

A data protection impact assessment ("DPIA") must be undertaken with assistance from the Data Protection Officer when there is systematic monitoring of a publicly accessible area on a large scale. If the DPIA suggests that the processing would result in a high risk to the rights and freedoms of individuals prior to any action being taken by the controller, the controller must consult the data protection authority.

During the course of consultation, the controller must provide information on the responsibilities of the controller and/or processors involved, the purpose of the intended processing, a copy of the DPIA, the safeguards provided by the GDPR to protect the rights and freedoms of data subjects and, where applicable, the contact details of the Data Protection Officer.

If the data protection authority is of the opinion that the CCTV monitoring would infringe the GDPR, it has to provide written advice to the controller within eight weeks of the request for a consultation and can use any of its wider investigative, advisory and corrective powers outlined in the GDPR.

**13.2 Are there limits on the purposes for which CCTV data may be used?**

Yes, there are limits to the purposes for which CCTV data may be used, especially:

- If CCTV films public roads, public places or facilities open to the public, prior authorisation of the local administrative authority in charge of security is required (i.e. "*le préfet du département*" or "*le préfet de police*", in Paris only).
- CCTV must not specifically be used to monitor employees, unless their daily task is critical (dealing with money, stock of high-value goods). CCTV must not film break rooms, rooms dedicated to unions, and toilets. Films cannot be kept for more than one month. Notices must be displayed on walls.

## 14 Employee Monitoring

**14.1 What types of employee monitoring are permitted (if any), and in what circumstances?**

Geolocalisation of vehicles driven by employees is permitted provided that:

(i) it is used only during the working time of the driver;
(ii) drivers are informed of the processing; and
(iii) personal data are kept for a period depending on the purpose of the processing.

Regarding the access control system, personal data cannot be stored for more than three months. A biometric system can only be used to protect access to sensitive places provided the controller has carried out a DPIA in accordance with article 35 of the GDPR.

The employer cannot monitor IT desk folders or emails of employees who have designated them as "personal/private".

Phone call recording is allowed but only for specific purposes, i.e. training or evaluation of employees.

**14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.**

Employees must be informed if the employer uses specific IT monitoring tools. No consent is required.

**14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?**

Works councils (social and economic councils) must advise the employer on issues related to the use of new technologies or any major changes within the company and can be consulted in this respect, pursuant to article. 2312-8 of the Labour Code.

## 15 Data Security and Data Breach

**15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?**

Yes. Personal data must be processed in a way that ensures security and safeguards against unauthorised or unlawful processing, accidental loss, destruction and damage of the data.

Both controllers and processors must ensure they have appropriate technical and organisational measures to meet the requirements of the GDPR. Depending on the security risk, this may include: the encryption of personal data; the ability to ensure the ongoing confidentiality, integrity and resilience of processing systems; an ability to restore access to data following a technical or physical incident; and a process for regularly testing and evaluating the technical and organisational measures for ensuring the security of processing.

**15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

The controller is responsible for reporting a personal data breach without undue delay (and in any case within 72 hours of first becoming aware of the breach) to the relevant data protection authority, unless the breach is unlikely to result in a risk to the rights and freedoms of the data subject(s). A processor must notify any data breach to the controller without undue delay.

The notification must include the nature of the personal data breach including the categories and number of data subjects concerned, the name and contact details of the Data Protection Officer or relevant point of contact, the likely consequences of the breach and the measures taken to address the breach including attempts to mitigate possible adverse effects.

**15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

Controllers have a legal requirement to communicate the breach to the data subject, without undue delay, if the breach is likely to result in a high risk to the rights and freedoms of the data subject.

The notification must include the name and contact details of the Data Protection Officer (or point of contact), the likely consequences of the breach and any measures taken to remedy or mitigate the breach.

The controller may be exempt from notifying the data subject if the risk of harm is remote (e.g., because the affected data is encrypted), the controller has taken measures to minimise the risk of harm (e.g., suspending affected accounts) or the notification requires a disproportionate effort (e.g., a public notice of the breach).

**15.4 What are the maximum penalties for data security breaches?**

The maximum penalty is the higher of €20 million or 4% of worldwide turnover.

## 16 Enforcement and Sanctions

**16.1 Describe the enforcement powers of the data protection authority(ies).**

(a) **Investigative Powers**: The data protection authority has wide powers to order the controller and the processor to

provide any information it requires for the performance of its tasks, to conduct investigations in the form of data protection audits, to carry out reviews on certificates issued pursuant to the GDPR, to notify the controller or processor of alleged infringement of the GDPR, to access all personal data and all information necessary for the performance of controllers' or processors' tasks and access to the premises of the data, including any data processing equipment. No criminal sanctions apply.

(b) **Corrective Powers**: The data protection authority has a wide range of powers including the ability to issue warnings or reprimands for non-compliance, to order the controller to disclose a personal data breach to the data subject, to impose a permanent or temporary ban on processing, to withdraw a certification and to impose an administrative fine (as below). No criminal sanctions apply.

(c) **Authorisation and Advisory Powers**: The data protection authority has a wide range of powers to advise the controller, accredit certification bodies and to authorise certificates, contractual clauses, administrative arrangements and binding corporate rules as outlined in the GDPR. No criminal sanctions apply.

(d) **Imposition of administrative fines for infringements of specified GDPR provisions**: The GDPR provides for administrative fines, which can be €20 million or up to 4% of the business' worldwide annual turnover of the preceding financial year. No criminal sanctions apply.

(e) **Non-compliance with a data protection authority**: The GDPR provides for administrative fines, which will be of €20 million or up to 4% of the business' worldwide annual turnover of the preceding financial year, whichever is higher. No criminal sanctions apply.

### 16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The GDPR entitles the CNIL to impose a temporary or definitive limitation including a ban on processing without court order.

### 16.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

CNIL may request any documents related to its investigation and access a business's IT network. It cannot access confidential information (e.g., privileged lawyer-client communications, journalistic sources or information relating to medical confidentiality).

On 18 February 2021, CNIL issued a warning to a sports club planning to use a facial recognition system to identify individuals subject to a commercial stadium ban. This warning follows several reports and investigations on the use of this technology.

### 16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

CNIL can exercise its powers against businesses established in other jurisdictions and must conduct a joint investigation with another EU supervisory authority in order to do so, in accordance with articles 60 to 67 of the GDPR.

## 17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

### 17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

The disclosure of personal data within the scope of a foreign discovery is possible, but only to the extent that such requests comply with certain rules: the request for personal data has to be for a legitimate purpose and respect professional secrecy; the communication of personal data shall be proportionate to the purpose of the discovery; the keeping of the communicated personal data in order to protect the rights attached to personal data; and the transfer of personal data shall respect the rules relating to the transfer of personal data outside France/the EU.

### 17.2 What guidance has/have the data protection authority(ies) issued?

In the last few months, CNIL has issued guidance regarding:

- cookies;
- processing of employees' personal data;
- the COVID-19 pandemic (especially the "TOUSANT-ICOVID" application by the French government); and
- connected devices.

## 18 Trends and Developments

### 18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

We have identified the following enforcement trends:

- monitoring GAFAM's compliance with personal data legislation (e.g. the Google and Amazon cases);
- commercial prospecting;
- cookies; and
- compliance with the security requirements of the GDPR.

### 18.2 What "hot topics" are currently a focus for the data protection regulator?

At the beginning of 2021, CNIL focused its investigations on the following areas:

- securing health personal data;
- geolocalisation; and
- cookies.

**Boriana Guimberteau** co-heads the IP/IT department of FTPA. She specialises in the protection, enforcement and infringement of IP rights and advises on all aspects of French and EU privacy and data protection law. She has particular expertise in the fashion, telecoms, media, tech, cosmetics and luxury sectors.
Before joining FTPA, Boriana gained valuable in-house experience having worked at LVMH (Perfume and Cosmetics division).
Her practice involves contentious and non-contentious matters.
Borianais a member of APRAM (Association of Legal Practitioners in Trademarks and Designs), the French group of the AIPPI and of the Brands and Innovation Committee of INTA (International Trademark Association – Enforcement Committee 2012–2013, Non-Traditional Trademarks Committee 2014–2015, Unreal Campaign Committee 2016–2017).

**Foucaud Tchekhoff Pochet et Associés (FTPA)**
1 Bis Avenue Foch
75116 Paris
France

Tel: +33 1 45 00 86 20
Email: bguimberteau@ftpa.fr
URL: https://ftpa.com

**Clémence Louvet** has been a member of the Paris Bar since 2019, and has practised in several law firms and entertainment companies, in particular in the luxury area.
Her practice encompasses advice and litigation in Intellectual Property and IT law, and she assists both domestic and international clients.
Clémence holds a postgraduate degree in Intellectual and Industrial Property from the University Panthéon-Assas (Paris II).

**Foucaud Tchekhoff Pochet et Associés (FTPA)**
1 Bis Avenue Foch
75116 Paris
France

Tel: +33 1 45 00 86 20
Email: clouvet@ftpa.fr
URL: https://ftpa.com

Foucaud Tchekhoff Pochet et Associés (FTPA) is an independent business law firm which brings together all the fundamental skills of business law in a multidisciplinary and multilingual team.
Our team works with clients from a wide range of industries, including software, fashion, pharmaceuticals and cosmetics. As such, we have developed extensive experience in intellectual property rights and technology law and act as both counsel and litigators on behalf of our clients. We assist our clients in the negotiation and drafting of all types of agreements (licensing agreements, assignment agreements, research and development agreements, coexistence agreements, IT agreements, website development agreements, etc.), and we support them in protecting their intangible assets and defend their interests in French and international litigation.

We also work with our clients in the area of personal data, helping them to comply with the applicable regulations in this area.

**https://ftpa.com**

# Germany


Dr. Bernhard Freund

Dr. Bernd Schmidt

PLANIT // LEGAL


## 1 Relevant Legislation and Competent Authorities

### 1.1 What is the principal data protection legislation?

Since 25 May 2018, the principal data protection legislation in the EU has been Regulation (EU) 2016/679 (the "**General Data Protection Regulation**" or "**GDPR**"). The GDPR repealed Directive 95/46/EC (the "**Data Protection Directive**") and has led to increased (though not total) harmonisation of data protection law across the EU Member States.

### 1.2 Is there any other general legislation that impacts data protection?

The GDPR leaves some areas for the Member States to regulate. Accordingly, the GDPR is complemented by the German Federal Data Protection Act ("***Bundesdatenschutzgesetz***" or "**BDSG**"), which applies to private and federal public entities. Furthermore, there are the Data Protection Acts of the 16 German states; however, these are only relevant to public entities on the state level.

### 1.3 Is there any sector-specific legislation that impacts data protection?

Yes, in some areas. Most notably, data protection in relation to electronic communications such as websites and apps is regulated by the EU ePrivacy Directive and the national legislation implementing it. The German legislator has presented the draft of a new law in this field (*Telekommunikation-Telemedien-Datenschutzgesetz* or "**TTDSG**"). Eventually, the EU ePrivacy Regulation will lead to further unification of the law; it was published as a draft in 2017 and is still in the legislative process. However, it is not expected to come into effect before 2023.

### 1.4 What authority(ies) are responsible for data protection?

Germany is a federal republic consisting of 16 states. Each state has its own data protection authority competent for the data processing activities of public and non-public entities within its territory. In addition, there is a federal data protection authority, which is primarily competent for federal public entities.

## 2 Definitions

### 2.1 Please provide the key definitions used in the relevant legislation:

- "**Personal Data**"
  This refers to any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- "**Processing**"
  This refers to any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- "**Controller**"
  This refers to the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- "**Processor**"
  This refers to a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
- "**Data Subject**"
  This refers to an individual who is the subject of the relevant personal data.
- "**Sensitive Personal Data**"
  This refers to personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health or sex life and sexual orientation, genetic data or biometric data.
- "**Data Breach**"
  This refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

## 3 Territorial Scope

**3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?**

The GDPR applies to businesses that are established in any EU Member State and that process personal data (either as a controller or processor, and regardless of whether or not the processing takes place in the EU) in the context of that establishment.

A business that is not established in any Member State but is subject to the laws of a Member State by virtue of public international law is also subject to the GDPR.

The GDPR applies to businesses outside the EU if they (either as controller or processor) process the personal data of EU residents in relation to: (i) the offering of goods or services (whether or not in return for payment) to EU residents; or (ii) the monitoring of the behaviour of EU residents (to the extent that such behaviour takes place in the EU).

Further, the GDPR applies to businesses established outside the EU if they monitor the behaviour of EU residents (to the extent that such behaviour takes place in the EU).

## 4 Key Principles

**4.1 What are the key principles that apply to the processing of personal data?**

- **Transparency**
  Personal data must be processed lawfully, fairly and in a transparent manner. Controllers must provide certain minimum information to data subjects regarding the collection and further processing of their personal data. Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
- **Lawful basis for processing**
  The processing of personal data is lawful only if, and to the extent that, it is permitted under EU data protection law. The GDPR provides an exhaustive list of legal bases on which personal data may be processed, of which the following are the most relevant for businesses: (i) prior, freely given, specific, informed and unambiguous consent of the data subject; (ii) contractual necessity (i.e., the processing is necessary for the performance of a contract to which the data subject is a party, or for the purposes of pre-contractual measures taken at the data subject's request); (iii) compliance with legal obligations (i.e., the controller has a legal obligation, under the laws of the EU or an EU Member State, to perform the relevant processing); or (iv) legitimate interests (i.e., the processing is necessary for the purposes of legitimate interests pursued by the controller, except where the controller's interests are overridden by the interests, fundamental rights or freedoms of the affected data subjects).
  Please note that businesses require stronger grounds to process sensitive personal data. The processing of sensitive personal data is only permitted under certain conditions, of which the most relevant for businesses are: (i) explicit consent of the affected data subject; (ii) the processing is necessary in the context of employment law; or (iii) the processing is necessary for the establishment, exercise or defence of legal claims.
- **Purpose limitation**
  Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes. If a controller wishes to use the relevant personal data in a manner that is incompatible with the purposes for which they were initially collected, it must: (i) inform the data subject of such new processing; and (ii) be able to rely on a lawful basis as set out above.
- **Data minimisation**
  Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed. A business should only process the personal data that it actually needs to process in order to achieve its processing purposes.
- **Retention**
  Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- **Data security**
  Personal data must be processed in a manner that ensures appropriate security of those data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

## 5 Individual Rights

**5.1 What are the key rights that individuals have in relation to the processing of their personal data?**

- **Right of access to data/copies of data**
  A data subject has the right to obtain from a controller the following information in respect of the data subject's personal data: (i) confirmation of whether, and where, the controller is processing the data subject's personal data; (ii) information regarding the purposes of the processing; (iii) information regarding the categories of data being processed; (iv) information regarding the categories of recipients with whom the data may be shared; (v) information regarding the period for which the data will be stored (or the criteria used to determine that period); (vi) information regarding the existence of the rights to erasure, rectification, restriction of processing and to object to processing; (vii) information regarding the existence of the right to complain to the relevant data protection authority; (viii) where the data were not collected from the data subject, information as to the source of the data; and (ix) information regarding the existence of, and an explanation of the logic involved in, any automated processing that has a significant effect on the data subject.
- **Right to rectification of errors**
  Controllers must ensure that inaccurate or incomplete data are erased or rectified. Data subjects have the right to rectification of inaccurate personal data.
- **Right to deletion/right to be forgotten**
  Data subjects have the right to erasure of their personal data (the "**right to be forgotten**") if: (i) the data are no longer needed for their original purpose (and no new lawful purpose exists); (ii) the lawful basis for the processing is the data subject's consent, the data subject withdraws that consent, and no other lawful ground exists; (iii) the data subject exercises the right to object, and the controller has no overriding grounds for continuing the processing; (iv) the data have been processed unlawfully; or (v) erasure is necessary for compliance with EU law or national data protection law.

- **Right to object to processing**
  Data subjects have the right to object, on grounds relating to their particular situation, to the processing of personal data where the basis for that processing is either public interest or legitimate interest of the controller. The controller must cease such processing unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the relevant data subject or requires the data in order to establish, exercise or defend legal rights.
- **Right to restrict processing**
  Data subjects have the right to restrict the processing of personal data, which means that the data may only be held by the controller, and may only be used for limited purposes if: (i) the accuracy of the data is contested (and only for as long as it takes to verify that accuracy); (ii) the processing is unlawful and the data subject requests restriction (as opposed to exercising the right to erasure); (iii) the controller no longer needs the data for their original purpose, but the data are still required by the controller to establish, exercise or defend legal rights; or (iv) verification of overriding grounds is pending, in the context of an erasure request.
- **Right to data portability**
  Data subjects have a right to receive a copy of their personal data in a commonly used machine-readable format and transfer their personal data from one controller to another or have the data transmitted directly between controllers.
- **Right to withdraw consent**
  A data subject has the right to withdraw their consent at any time. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject must be informed of the right to withdraw consent. It must be as easy to withdraw consent as to give it.
- **Right to object to marketing**
  Data subjects have the right to object to the processing of personal data for the purpose of direct marketing, including profiling.
- **Right to complain to the relevant data protection authority(ies)**
  Data subjects have the right to lodge complaints concerning the processing of their personal data with the data protection authority of their region (*Bundesland*) or the data protection authority competent for the relevant data controller/processor, provided the data subjects live in Germany or the alleged infringement occurred in Germany.
- **Right to basic information**
  Data subjects have the right to be provided with information on the identity of the controller, the reasons for processing their personal data and other relevant information necessary to ensure the fair and transparent processing of personal data.

## 6 Registration Formalities and Prior Approval

**6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?**

No, processing activities do not have to be registered with the supervisory authority. Only the contact details of the data protection officer must be communicated to the supervisory authority.

**6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?**

This is not applicable to Germany.

**6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?**

This is not applicable to Germany.

**6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?**

This is not applicable to Germany.

**6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?**

This is not applicable to Germany.

**6.6 What are the sanctions for failure to register/notify where required?**

This is not applicable to Germany.

**6.7 What is the fee per registration/notification (if applicable)?**

This is not applicable to Germany.

**6.8 How frequently must registrations/notifications be renewed (if applicable)?**

This is not applicable to Germany.

**6.9 Is any prior approval required from the data protection regulator?**

This is not applicable to Germany.

**6.10 Can the registration/notification be completed online?**

This is not applicable to Germany.

**6.11 Is there a publicly available list of completed registrations/notifications?**

This is not applicable to Germany.

**6.12 How long does a typical registration/notification process take?**

This is not applicable to Germany.

## 7 Appointment of a Data Protection Officer

**7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.**

The appointment of a Data Protection Officer for controllers or processors is only mandatory in some circumstances, including where there is: (i) large-scale regular and systematic monitoring of individuals; (ii) large-scale processing of sensitive personal data; (iii) processing of personal data requiring a data protection impact assessment; or (iv) professional processing of personal data for the purpose of transfer, anonymised transfer or market or opinion research. Furthermore, a Data Protection Officer must be appointed if constantly at least 20 persons are concerned with the automated processing of personal data.

Where a business designates a Data Protection Officer voluntarily, the requirements of the GDPR apply as though the appointment were mandatory.

**7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?**

In the circumstances where appointment of a Data Protection Officer is mandatory, failure to comply may result in the wide range of penalties available under the GDPR.

**7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?**

The appointed Data Protection Officer should not be dismissed or penalised for performing their tasks and should report directly to the highest management level of the controller or processor.

**7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?**

A single Data Protection Officer is permitted by a group of undertakings provided that the Data Protection Officer is easily accessible from each establishment.

**7.5 Please describe any specific qualifications for the Data Protection Officer required by law.**

The Data Protection Officer should be appointed on the basis of professional qualities and should have an expert knowledge of data protection law and practices. While this is not strictly defined, it is clear that the level of expertise required will depend on the circumstances. For example, the involvement of large volumes of sensitive personal data will require a higher level of knowledge.

**7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?**

A Data Protection Officer should be involved in all issues which relate to the protection of personal data. The GDPR outlines the minimum tasks required by the Data Protection Officer, which include: (i) informing the controller, processor and their relevant employees who process data of their obligations under the GDPR; (ii) monitoring compliance with the GDPR, national data protection legislation and internal policies in relation to the processing of personal data including internal audits; (iii) advising on data protection impact assessments and the training of staff; and (iv) co-operating with the data protection authority and acting as the authority's primary contact point for issues related to data processing.

**7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?**

Yes; the controller or processor must notify the data protection authority of the contact details of the designated Data Protection Officer.

**7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?**

The Data Protection Officer does not necessarily need to be named in the public-facing privacy notice. However, the contact details of the Data Protection Officer must be notified to the data subject when personal data relating to that data subject are collected. As a matter of good practice, the Article 29 Working Party (the "**WP29**") (now the European Data Protection Board (the "**EDPB**")) recommended in its 2017 guidance on Data Protection Officers that both the data protection authority and employees should be notified of the name and contact details of the Data Protection Officer.

## 8 Appointment of Processors

**8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?**

Yes; the business that appoints a processor to process personal data on its behalf is required to enter into an agreement with the processor which sets out the subject matter and duration of the processing, the nature and purpose of the processing, the types of personal data and categories of data subjects and the obligations and rights of the controller (i.e., the business).

It is essential that the processor appointed by the business complies with the GDPR.

**8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?**

The processor must be appointed under a binding agreement in writing (including electronic form). The contractual terms

must stipulate that the processor: (i) only acts on the documented instructions of the controller; (ii) imposes confidentiality obligations on all employees; (iii) ensures the security of personal data that it processes; (iv) abides by the rules regarding the appointment of sub-processors; (v) implements measures to assist the controller with guaranteeing the rights of data subjects; (vi) assists the controller in obtaining approval from the relevant data protection authority; (vii) either returns or destroys the personal data at the end of the relationship (except where required by EU or Member State law); and (viii) provides the controller with all information necessary to demonstrate compliance with the GDPR.

## 9 Marketing

**9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).**

Marketing by email, SMS or fax requires explicit prior consent. As an exception, marketing using email addresses acquired in the context of a sale is permitted if (i) the marketing concerns similar goods or services of the seller, (ii) the buyer has not objected to the use of the email address for marketing, and (iii) the buyer is reminded of the right to object when providing the email address and in each marketing email.

**9.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?**

These restrictions also apply in a business-to-business context.

**9.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).**

Marketing by phone in a business-to-consumer context requires explicit prior consent; however, in a business-to-business context, it requires presumed consent. Marketing via post is generally accepted unless the recipients have objected. It is recommended not to send postal marketing to persons having registered for the "Robinson list" maintained by the German dialogue marketing association (*Deutscher Dialogmarketing Verband*).

**9.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?**

Yes; the restrictions noted above also apply to marketing sent from other jurisdictions.

**9.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?**

Yes; in particular, the data protection authorities investigate complaints made by recipients of marketing communications. This has repeatedly led to administrative fines. For example, a health insurance company was fined €1.24 million by the data protection authority of Baden-Wuerttemberg for not having taken proper measures to prevent marketing emails being sent to persons who did not consent.

**9.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?**

Selling and purchasing marketing lists is not unlawful *per se*. It must be carefully assessed whether there is a legitimate basis for the collection and use of the personal data for marketing purposes under the GDPR (e.g., clear and well-documented consent of each data subject). Furthermore, other requirements such as transparency to the data subjects must be observed.

**9.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?**

The maximum penalty is €20 million or 4% of the global annual turnover (whichever is higher).

## 10 Cookies

**10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).**

Pursuant to Article 5 of the EU ePrivacy Directive, the storage of cookies (or other data) on an end user's device requires prior consent (the applicable standard of consent is derived from the GDPR). In order for consent to be valid, it must be informed, specific, freely given and must constitute a real and unambiguous indication of the individual's wishes. This does not apply if: (i) the cookie is for the sole purpose of carrying out the transmission of a communication over an electronic communications network; or (ii) the cookie is strictly necessary to provide an "information society service" (e.g., a service over the internet) requested by the subscriber or user and is thus essential to fulfil their request.

The German government claims that Article 5 of the ePrivacy Directive was properly implemented by the pre-existent German Telemedia Act ("**TMG**"), which is quite controversial. The draft TTDSG will, once passed, provide much clearer rules on cookies in line with the EU ePrivacy legislation.

The EU Commission intends to pass a new ePrivacy Regulation that will replace the respective national legislation in the EU Member States. The ePrivacy Regulation is still in the legislative process and is not expected to come into force before 2023.

**10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?**

The purpose of the cookie is the deciding factor. Cookies which are considered strictly necessary to provide the service (i.e. the website) do not require consent, such as a cookie used to store the content of a shopping cart while shopping online, or a session cookie maintaining the "log-in" status on a website with a log-in functionality.

"Strictly necessary" cookies will tend to be both first-party and session cookies. In contrast, third-party cookies and persistent cookies, such as tracking cookies, typically require consent.

**10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?**

Yes; the German data protection authorities have investigated the use of cookies on websites not only when responding to complaints, but also pro-actively. For example, in a concerted action in the autumn of 2020, they sent out questionnaires on cookies and web-tracking to several news websites. There have also been cases where administrative fines were issued.

**10.4 What are the maximum penalties for breaches of applicable cookie restrictions?**

See question 9.7 above.

## 11 Restrictions on International Data Transfers

**11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.**

Data transfers to other jurisdictions that are not within the European Economic Area (the "**EEA**") can only take place if the transfer is to an "Adequate Jurisdiction" (as specified by the EU Commission), the business has implemented one of the required safeguards as specified by the GDPR, or one of the derogations specified in the GDPR applies to the relevant transfer. The EDPB Guidelines (2/2018) set out that a "layered approach" should be taken with respect to these transfer mechanisms. If the transfer is not to an Adequate Jurisdiction, the data exporter should first explore the possibility of implementing one of the safeguards provided for in the GDPR before relying on a derogation.

**11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).**

When transferring personal data to a country other than an Adequate Jurisdiction, businesses must ensure that there are appropriate safeguards on the data transfer, as prescribed by the GDPR. The GDPR offers several ways to ensure compliance for international data transfers, one of which is consent of the relevant data subject. Other common options are the use of Standard Contractual Clauses ("**SCCs**") or Binding Corporate Rules ("**BCRs**").

Businesses can adopt the SCCs drafted by the EU Commission – these are available for transfers between controllers, as well as transfers between a controller (as exporter) and a processor (as importer). International data transfers may also take place on the basis of contracts agreed between the data exporter and data importer provided that they conform to the protections outlined in the GDPR, and they have prior approval from the relevant data protection authority.

International data transfers within a group of businesses can be safeguarded by the implementation of BCRs. The BCRs will always need approval from the relevant data protection authority. Most importantly, the BCRs will need to include a mechanism to ensure they are legally binding and enforced by every member in the group of businesses. Among other things, the BCRs must set out the group structure of the businesses, the proposed data transfers as well as their purpose, the rights of data subjects, the mechanisms that will be implemented to ensure compliance with the GDPR and the relevant complainant procedures.

For the transfer of personal data to the USA, there historically was an additional transfer mechanism based on the EU-US Privacy Shield Framework. This is no longer available, as the respective decision of the EU Commission has been invalidated by the European Union Court of Justice ("**CJEU**") in *Schrems II* (Case C-311/18) on 16 July 2020. Moreover, on account of the "invasive" surveillance programme maintained by the USA, the CJEU has stipulated stricter requirements for the transfer of personal data to the USA, by demanding "additional safeguards" on top of the need for SCC or BCR. These stricter requirements also apply to other non-EEA countries with similar surveillance programmes. See also question 11.4.

**11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.**

Specific data transfers that are based on an adequacy decision, BCR, SCC or on one of the derogations for specific situations (Art. 49(1) GDPR, first subparagraph) do not require registration/notification or prior approval. However, BCR as such require initial approval from the data protection authority.

Prior approval by the competent supervisory authority is required for data transfers based on contractual clauses other than the SCC (so-called "*ad hoc* clauses"). Further, when relying on the derogation of "compelling legitimate interests" (Art. 49(1) GDPR, second subparagraph), the data controller must inform the supervisory authority of the transfer.

**11.4 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?**

The EDPB has adopted the Recommendations 01/2020 on measures that supplement transfer tools such as the BCR and SCC to ensure the requirements set out by the CJEU in *Schrems II* are met. At the time of writing, those Recommendations are open for public consultation and subject to revision.

**11.5 What guidance (if any) has/have the data protection authority(ies) issued in relation to the European Commission's revised Standard Contractual Clauses?**

The EU Commission has adopted new SCCs on June 4, 2021. In relation to the draft of those SCCs, the EDPB and the European Data Protection Supervisor have issued Joint Opinion 1/2021.

## 12 Whistle-blower Hotlines

**12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?**

Internal whistle-blowing schemes are generally established in pursuance of a concern to implement proper corporate governance principles in the daily functioning of businesses. Whistle-blowing is designed as an additional mechanism for employees to report misconduct internally through a specific channel and supplements a business' regular information and reporting channels, such as employee representatives, line management, quality-control personnel or internal auditors who are employed precisely to report such misconducts.

The WP29 has limited its Opinion 1/2006 on the application of EU data protection rules to internal whistle-blowing schemes to the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime. The scope of corporate whistle-blower hotlines, however, does not need to be limited to particular issues. In the Opinion, it is recommended that the business responsible for the whistle-blowing scheme should carefully assess whether it might be appropriate to limit the number of persons eligible for reporting alleged misconduct through the whistle-blowing scheme and whether it might be appropriate to limit the number of persons who may be reported through the scheme, in particular in light of the seriousness of the alleged offences reported.

The EU has introduced Directive (EU) 2019/1937 ("**Whistleblower Directive**") in 2019. This legislation must be implemented into Member State law by 17 December 2021 (partly by 17 December 2023). It introduces an obligation to establish internal reporting channels for public entities and private entities with 50 or more workers. The scope of such reporting channels must cover a broad range of breaches of EU law, including data protection law.

**12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?**

Anonymous reporting is not prohibited under EU data protection law; however, it raises problems as regards the essential requirement that personal data should only be collected fairly. In Opinion 1/2006, the WP29 considered that only identified reports should be advertised in order to satisfy this requirement. Businesses should not encourage or advertise the fact that anonymous reports may be made through a whistle-blower scheme.

An individual who intends to report to a whistle-blowing system should be aware that he/she will not suffer due to his/her action. The whistle-blower, at the time of establishing the first contact with the scheme, should be informed that his/her identity will be kept confidential during all stages of the process, and in particular will not be disclosed to third parties, such as the incriminated person or to the employee's line management. If, despite this information, the person reporting to the scheme still wants to remain anonymous, the report will be accepted into the scheme. Whistle-blowers should be informed that their identity may need to be disclosed to the relevant people involved in any further investigation or subsequent judicial proceedings instigated as a result of any enquiry conducted by the whistle-blowing scheme.

The EU Whisteblower Directive (see question 11.1) explicitly leaves it to the Member States to decide in their implementation acts whether legal entities are required to accept or follow up on anonymous reports of breaches. The current draft of the German implementation act (*Hinweisgeberschutzgesetz*) does not include an obligation to accept anonymous reports, but does not prohibit accepting anonymous reports either.

## 13 CCTV

**13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?**

A data protection impact assessment ("**DPIA**") must be undertaken with assistance from the Data Protection Officer when there is systematic monitoring of a publicly accessible area on a large scale. If the DPIA suggests that the processing would result in a high risk to the rights and freedoms of individuals prior to any action being taken by the controller, the controller must consult the data protection authority.

During the course of a consultation, the controller must provide information regarding the responsibilities of the controller and/or processors involved, the purpose of the intended processing, a copy of the DPIA, the safeguards provided by the GDPR to protect the rights and freedoms of data subjects and where applicable, the contact details of the Data Protection Officer.

If the data protection authority is of the opinion that the CCTV monitoring would infringe the GDPR, it must provide written advice to the controller within eight weeks of the request of a consultation and can use any of its wider investigative, advisory and corrective powers outlined in the GDPR.

As part of the transparency requirements, CCTV recording of public areas requires visible signs indicating at least the name and contact details of the data controller and a reference to further information. The German data protection authorities have issued templates for CCTV signs, which are based on templates endorsed by the EDPB but more comprehensive.

**13.2 Are there limits on the purposes for which CCTV data may be used?**

As far as the CCTV data contains personal data, processing of the data for any purpose requires a legal basis according to the GDPR. Whether a sufficient legal basis can be found strongly depends on the purpose pursued. For example, CCTV is often used to protect the property of a company against theft and vandalism, or to protect the employees and visitors against assault; these purposes may constitute legitimate interests that justify the processing if they are not overridden by the interests of the persons being recorded. In contrast, monitoring the effectiveness of employees via CCTV is typically not justifiable under the GDPR and the BDSG.

## 14 Employee Monitoring

**14.1 What types of employee monitoring are permitted (if any), and in what circumstances?**

The processing of personal data relating to employees is only permitted if the processing is necessary for the establishment,

performance or termination of the employment relationship. Any employee monitoring must be checked against this standard, on a case-by-case basis, considering all circumstances. For example, simple time recording is typically permitted as it is in principle required to monitor basic compliance with the employment contract and may also be required for invoicing services to clients. On the other hand, the ability for an employer to use silent monitoring in call-centres is limited, as this can easily create a disproportionate "surveillance pressure" for the agents.

**14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.**

Where the monitoring has no statutory basis, consent would be required. However, due to the asymmetrical relationship between employer and employee, there is an increased risk that consent may not be regarded as freely given and, thus, would be invalid. Therefore, it is essential to ensure that withholding consent has no negative consequences for the employees. Furthermore, the employee(s) must be made aware that consent can be withdrawn at any time. For these reasons, in practice, employee monitoring can rarely be based on consent.

The employer as a data controller has transparency obligations towards the employees with regard to any processing of their personal data, including employee monitoring. The information must be provided in advance, e.g., during onboarding or via an employee privacy notice on the company's intranet.

**14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?**

Employee monitoring is subject to co-determination rights as far as it relies on technical devices. Therefore, if the company has a works council, the prior approval of the works council must be obtained to introduce employee monitoring.

## 15 Data Security and Data Breach

**15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?**

Yes; personal data must be processed in a way which ensures security and safeguards against unauthorised or unlawful processing, accidental loss, destruction and damage of the data.

Both controllers and processors must ensure they have the appropriate technical and organisational measures to meet the requirements of the GDPR. Depending on the security risk, this may include: the encryption of personal data; the ability to ensure ongoing confidentiality, integrity and resilience of processing systems; an ability to restore access to data following a technical or physical incident; and a process for regularly testing and evaluating the technical and organisational measures for ensuring the security of processing.

**15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

The controller is responsible for reporting a personal data breach without undue delay (and in any case within 72 hours of first becoming aware of the breach) to the relevant data protection authority, unless the breach is unlikely to result in a risk to the rights and freedoms of the data subject(s). A processor must notify any data breach to the controller without undue delay.

The notification must include the nature of the personal data breach including the categories and number of data subjects concerned, the name and contact details of the Data Protection Officer or relevant point of contact, the likely consequences of the breach and the measures taken to address the breach including attempts to mitigate possible adverse effects.

**15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

Controllers have a legal requirement to communicate the breach to the data subject, without undue delay, if the breach is likely to result in a high risk to the rights and freedoms of the data subject.

The notification must include the name and contact details of the Data Protection Officer (or point of contact), the likely consequences of the breach and any measures taken to remedy or mitigate the breach.

The controller may be exempt from notifying the data subject if the risk of harm is remote (e.g., because the affected data is encrypted), the controller has taken measures to minimise the risk of harm (e.g., suspending affected accounts) or the notification requires a disproportionate effort (in which case data subjects must be made aware via a public communication).

**15.4 What are the maximum penalties for data security breaches?**

The maximum penalty is €20 million or 4% of worldwide turnover (whichever is higher).

## 16 Enforcement and Sanctions

**16.1 Describe the enforcement powers of the data protection authority(ies).**

(a) **Investigative Powers**: The data protection authority has wide powers to order the controller and the processor to provide any information it requires for the performance of its tasks, to conduct investigations in the form of data protection audits, to carry out review on certificates issued pursuant to the GDPR, to notify the controller or processor of alleged infringement of the GDPR, to access all personal data and all information necessary for the performance of controllers' or processors' tasks and access to the premises of the data including any data processing equipment. No criminal sanctions apply.

(b) **Corrective Powers**: The data protection authority has a wide range of powers including to issue warnings or reprimands for non-compliance, to order the controller to disclose a personal data breach to the data subject, to impose a permanent or temporary ban on processing, to withdraw a certification and to impose an administrative fine (as below). No criminal sanctions apply.

(c) **Authorisation and Advisory Powers**: The data protection authority has a wide range of powers to advise the controller, accredit certification bodies and to authorise certificates, contractual clauses, administrative arrangements and binding corporate rules as outlined in the GDPR. No criminal sanctions apply.

(d) **Imposition of administrative fines for infringements of specified GDPR provisions**: The GDPR provides for administrative fines which can be €20 million or up to 4% of the business' worldwide annual turnover of the preceding financial year, whichever is higher. The GDPR does not provide for criminal sanctions. However, the BDSG contains a provision that allows for criminal sanctions based on the unlawful processing of personal data; however, such sanctions have been rarely enforced.

(e) **Non-compliance with a data protection authority**: The GDPR provides for administrative fines which will be €20 million or up to 4% of the business' worldwide annual turnover of the preceding financial year, whichever is higher. No criminal sanctions apply.

**16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?**

The GDPR entitles the relevant data protection authority to impose a temporary or definitive limitation including a ban on processing.

**16.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.**

Administrative proceedings often follow a data subject making a complaint against the data controller. However, the authorities may also pro-actively initiate investigations, e.g., following media reports. In case of formal proceedings, the data controller will receive a written notice setting out the known facts and the alleged violation of data protection law, inviting the controller to comment. If the violations were not intentional, it is often possible to avoid fines provided the controller is co-operative and adapts the processing as demanded by the authority.

In case of more severe violations, the authorities may issue fines. The German data protection authorities have agreed on a controversial model to determine the cost of fines based on the turnover of the data controller, the severity of the violation and a number of other factors. Some larger fines issued according to this model have successfully been challenged in courts.

The Hamburg Commissioner for Data Protection found in 2020 that a German service centre of the clothing retail company H&M had in a number of cases meticulously gathered data about the private life, health conditions and religious beliefs of employees as a basis for decisions in the context of the employment relationship. The authority, having read media articles about the practice, demanded to "freeze" and hand over the data. The company handed over the data, which was evaluated by the authority. Ultimately, a fine of almost €35.3 million was issued.

More recently, the German data protection authorities have announced that, in the aftermath of the *Schrems II* case, they will be sending out questionnaires in 2021 to selected companies relating to international data transfers (including questionnaires on website tracking, email servers and intra-group data transfers). This may lead to subsequent enforcement activities.

**16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?**

Yes; however, cases like this are rare and enforcement may prove difficult. One example is the "urgency procedure" (Art. 66 GDPR) initiated by the Hamburg Data Protection Commissioner in April 2021 against Facebook Ireland Ltd. The authority issued an injunction against Facebook not to collect data from users of WhatsApp and/or to process such data for purposes of Facebook.

In terms of enforcement, controllers or processors not established in the EU but being subject to GDPR must appoint an EU Representative. One recital of the GDPR contemplates that this EU Representative could be subject to enforcement proceedings in the event of non-compliance by the controller or processor (Recital 80(6) GDPR). However, this has had little practical relevance so far.

## 17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

**17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?**

Requests within the EU/EEA can be based on mutual assistance treaties and may then be processed similarly to requests by domestic agencies. Still, the data controller must assess whether there is a legal basis for disclosure (e.g., a binding obligation to disclose data under EU or Member State law).

For requests made from outside the EU/EEA, the data controller must determine (i) whether there is a legal basis under the GDPR to disclose the data (e.g., a legitimate interest in complying with the request if there are no overriding interests of the data subjects), and (ii) if the conditions for data transfers to non-EU countries are fulfilled. Regarding (i), it must be noted that any foreign judgment or decision is not recognised or enforceable under the GDPR unless based on a mutual legal assistance treaty. For example, US disclosure orders have no formal effect in the EU and are therefore no sufficient basis for disclosure *per se* (while the legitimate interest in complying with such orders *may* be a sufficient basis). Regarding (ii), one of the recognised transfer mechanisms must be used or a derogation must apply (such as the establishment, exercise or defence of legal claims, Art. 49(1)(e) GDPR).

It follows from the above that requests must be assessed carefully on a case-by-case basis.

### 17.2 What guidance has/have the data protection authority(ies) issued?

Some guidance on pre-trial discovery can be found in Guidelines 2/2018 of the EDPB. The working document 158 of the Art.-29-Working Party on pre-trial discovery, although issued before the GDPR, also sets out helpful guidance regarding how to address conflicts between foreign disclosure requests and EU data protection law.

## 18 Trends and Developments

### 18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

The statistics indicate that while the number of published cases per month has remained constant over the last year, the total amount of fines issues since the GDPR has entered into force has risen dramatically within the EU. It has almost tripled from €100 million a year ago to €300 million as of May 2021. This demonstrates an increasing willingness of data protection authorities to issue very large fines in selected cases. This effect has also been strongly felt in Germany, notably with fines of €35.3 million (*Hamburg Data Protection Commissioner vs H&M in October 2020*) and €10.4 million (*State Commissioner for Data Protection of Lower Saxony vs notebooksbilliger.de*).

### 18.2 What "hot topics" are currently a focus for the data protection regulator?

The implementation of *Schrems II*, requiring additional safeguards for data transfers to the USA and some other non-EU countries, is still very much on the agenda. The German authorities have built a taskforce, developed questionnaires on international data transfers and announced that they will be sending these out to companies in the course of the year.

**Dr. Bernhard Freund** is a founding partner of PLANIT // LEGAL. He advises on data protection and IT law and is appointed as an external Data Protection Officer by various companies. Clients value in particular the combination of his legal and technical expertise.
Bernhard is a certified IT lawyer (*Fachanwalt für IT-Recht*) with an academic background in artificial intelligence. He consults where the legal and tech perspectives meet – such as innovations in AI, legal tech, blockchain, smart contracts, DeFi and data-driven business models. Data protection is another focus of his. He is certified as CIPP/E.
Before founding PLANIT // LEGAL, Bernhard worked as a software developer, as a legal clerk for the Hamburg Data Protection Commissioner and as a lawyer at an international law firm. Bernhard was also associate professor (*Lehrbeauftragter*) for data protection law at the Hamburg University of Applied Sciences and currently is a trainer with the PLANIT // Academy.

**PLANIT // LEGAL**
Jungfernstieg 1
20095 Hamburg
Germany

Tel: +49 40 609 44 190
Email: bernhard.freund@planit.legal
URL: www.planit.legal

**Dr. Bernd Schmidt** is a founding partner of PLANIT // LEGAL. He advises on data protection and IT law and is assigned as a Data Protection Officer for various companies. Clients value in particular his data protection experience and his hands-on advisory approach.
Bernd is a certified IT lawyer (*Fachanwalt für IT-Recht*) and certified data protection expert (GDD cert. and CIPP/E). He regularly publishes on data protection and IT law matters.
Before founding PLANIT // LEGAL, Bernd worked as an attorney-at-law in the Munich office of Bird & Bird and in a boutique law firm for data protection law. He has working experience from the Hamburg Data Protection Authority (*Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit*) and the IT/IP groups of Taylor Wessing (Hamburg) and Simonsen Advkatfirma (Oslo).
Bernd is member of the EuroPrivacy Certification Board of Experts and teaches IT law at the University of Bremen.
Bernd is fluent in German, English and Norwegian.

**PLANIT // LEGAL**
Jungfernstieg 1
20095 Hamburg
Germany

Tel: +49 40 609 44 190
Email: bernd.schmidt@planit.legal
URL: www.planit.legal

PLANIT // LEGAL is a boutique law firm offering comprehensive advice on German and European IT and data protection law. We are on your side either supporting your legal, data protection and compliance departments or serving as external data protection officers.
Our services cover all matters of IT law, including software licenses, IT outsourcing, e-commerce, data protection, IT security and due diligence. We develop solutions that fit your company – be it by drafting contracts, supporting IT projects or representing your interests in disputes with supervisory authorities or in court.
At PLANIT // LEGAL, we combine excellence in the field of law with a deep understanding of technology and the innovations that drive modern IT. Technology is our passion. We are pragmatic, competent and clear-cut. We also have a strong network and work closely with colleagues from other jurisdictions and specialisations.

**www.planit.legal**

PLANIT // LEGAL

# Greece


Dr. Nikos Th. Nikolinakos


Dina Th. Kouvelou


Alexis N. Spyropoulos

Nikolinakos & Partners Law Firm

## 1 Relevant Legislation and Competent Authorities

### 1.1 What is the principal data protection legislation?

Since 25 May 2018, the principal data protection legislation in the EU has been Regulation (EU) 2016/679 (the General Data Protection Regulation or GDPR). The GDPR repealed Directive 95/46/EC (Data Protection Directive) and has led to increased (though not total) harmonisation of data protection law across the EU Member States.

Since 29 August 2019, the main data protection legislation in Greece has been Law 4624/2019, which has implemented Regulation (EU) 2016/679 (GDPR) and incorporated Directive (EU) 2016/680. Law 4624/2019 repealed Law 2472/1997, which incorporated Directive 95/46/EC.

### 1.2 Is there any other general legislation that impacts data protection?

Law 3471/2006, which incorporates Directive 2002/58/EC (E-Privacy Directive) – as amended by Directive 2006/13/EC – is complementary and specific to the institutional framework for the protection of personal data in the field of electronic communications.

### 1.3 Is there any sector-specific legislation that impacts data protection?

Provisions of data protection are further dispersed across various Greek laws:

- Law 4579/2018 sets obligations on air operators regarding passengers' details;
- Law 4577/2018, transposing the NIS Directive (EU 2016/1148), imposes obligations for system and network security on businesses in the fields of energy, transport, credit, financial infrastructure, health, water and digital infrastructure, e-commerce and information society services;
- Law 3917/2011 regulates the retention of data that is produced or processed based on the provision of publicly available electronic communication services or public communication networks, use of audio or video surveillance systems in public places;
- Law 3783/2009 sets the framework for collection and storage of identification data of mobile services subscribers for national security reasons and for the identification of particularly serious crimes; and
- article 8 of Law 3144/2003 sets requirements of processing of workers' medical data.

### 1.4 What authority(ies) are responsible for data protection?

The Hellenic Data Protection Authority (HDPA) is a constitutionally established independent public authority that serves as the watchdog for the application and enforcement of the data protection legislation.

Moreover, the Hellenic Authority for Communication Security and Privacy (ADAE) is responsible for the protection of free correspondence and communication, including personal data issues in telecommunications.

## 2 Definitions

### 2.1 Please provide the key definitions used in the relevant legislation:

- "**Personal Data**"
  This means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- "**Processing**"
  This means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

- "**Controller**"
  This means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- "**Processor**"
  This means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
- "**Data Subject**"
  This means an individual who is the subject of the relevant personal data.
- "**Sensitive Personal Data**"
  This includes personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health or sex life and sexual orientation, genetic data or biometric data.
- "**Data Breach**"
  This means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

## 3 Territorial Scope

### 3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The GDPR applies to businesses that are established in any EU Member State, and that process personal data (either as a controller or processor, and regardless of whether the processing takes place in the EU or not) in the context of that establishment.

A business that is not established in any Member State but is subject to the laws of a Member State by virtue of public international law is also subject to the GDPR.

The GDPR applies to businesses outside the EU if they (either as controller or processor) process the personal data of EU residents in relation to: (i) the offering of goods or services (whether or not in return for payment) to EU residents; or (ii) the monitoring of the behaviour of EU residents (to the extent that such behaviour takes place in the EU).

Further, the GDPR applies to businesses established outside the EU if they monitor the behaviour of EU residents (to the extent such behaviour takes place in the EU).

## 4 Key Principles

### 4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  Personal data must be processed lawfully, fairly and in a transparent manner.
- **Lawful basis for processing**
  The GDPR provides an exhaustive list of legal bases on which personal data may be processed, of which the following are the most relevant for businesses: (i) prior, freely given, specific, informed and unambiguous consent of the data subject; (ii) contractual necessity; (iii) compliance with the controller's legal obligations; or (iv) the controller's legitimate interests, except where they are overridden by the interests, fundamental rights or freedoms of the data subjects).

  Please note that the processing of sensitive personal data is only permitted under certain conditions, of which the most relevant for businesses are: (i) explicit consent provided by the data subject; (ii) the processing is necessary under employment law provisions; (iii) the processing is necessary for the establishment, exercise or defence of legal claims; or (iv) the data have already been disclosed publicly.
- **Purpose limitation**
  Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with them. If a controller wishes to use the relevant personal data in a manner that is incompatible with the initial purposes, the data subject must be informed beforehand; and a lawful basis of processing must be provided.
- **Data minimisation**
  Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed.
- **Retention**
  Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be retained for longer periods of time if they have been stored, for the purposes of scientific or historical research or for statistical purposes in the public's interest and provided that the appropriate technical and organisational measures are applied.
- **Accuracy**
  Personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that inaccurate personal data are erased or rectified without delay.
- **Data security**
  Personal data must be processed in a manner that ensures their security, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage.
- **Accountability**
  The controller is responsible for, and must be able to demonstrate compliance with the data protection principles.

## 5 Individual Rights

### 5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**
  Data subjects have the right to obtain from controllers information regarding: (i) the purposes and the location of the processing; (ii) the categories of data being processed; (iii) the categories of recipients with whom the data may be shared; (iv) the period for which the data will be stored; (v) the existence of the rights to erasure, rectification, restriction of processing and to object to processing; (vi) the existence of the right to complain to the relevant data protection authority; (vii) the source of the data, if they have not been collected from the data subject; and (viii) the existence of, and an explanation of the logic involved in, any automated processing that has a significant effect on the data subject.
  Access to data may be denied when the exceptions provided in article 33 of Law 4624/2019 are applicable. A copy of the personal data undergoing processing can be provided upon request to the data subject.

- **Right to rectification of errors**
  Data subjects have the right to have inaccurate or incomplete personal data erased, rectified, or completed.
- **Right to deletion/right to be forgotten**
  Data subjects have this right in situations where: (i) the data are no longer needed for their original purpose; (ii) the data subject has withdrawn its consent for the processing, and no other lawful ground exists; (iii) the data subject exercises the right to object, and the controller has no overriding grounds for continuing the processing; (iv) the data have been processed unlawfully; or (v) erasure is necessary for compliance with EU or national data protection law. Article 17 GDPR provides a list of exceptions, where the data subjects are refused the deletion of their data. Additionally, article 33 of Law 4624/2019 stipulates that if certain conditions are met, the deletion of the data may be replaced by the mere restriction of their processing.
- **Right to object to processing**
  Data subjects have the right to object, on grounds relating to their particular situation, to the processing of personal data where the basis for that processing is either the public interest or the legitimate interest of the controller. The controller must cease such processing unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or requires the data in order to establish, exercise or defend legal rights.
  Law 4624/2019 provides that when a public body is concerned or the processing of the data is conducted for the purposes of scientific or historical research or for statistical purposes, provided that certain conditions are met, the right to object does not apply.
- **Right to restrict processing**
  The right to restrict processing means that the data may only be held by the controller, and may only be used for limited purposes if: (i) the accuracy of the data is contested (and only for as long as it takes to verify that accuracy); (ii) the processing is unlawful and the data subject requests restriction; (iii) the controller no longer needs the data for their original purpose, but the data are still required by the controller to establish, exercise or defend legal rights; or (iv) verification of overriding grounds is pending, in the context of an erasure request. Should at any point the restriction be lifted the controller informs the data subjects.
- **Right to data portability**
  Data subjects have a right to receive a copy of their personal data in a commonly used machine-readable format and transfer their personal data from one controller to another or have the data transmitted directly between controllers.
- **Right to withdraw consent**
  Data subjects may withdraw their consent at any time. This withdrawal does not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject must be informed of this right. It must be as easy to withdraw consent as to give it.
- **Right to object to marketing**
  Data subjects have the right to object to the processing of personal data for the purpose of direct marketing, including profiling.
- **Right to complain to the relevant data protection authority(ies)**
  Data subjects have the right to lodge complaints concerning the processing of their personal data with the Hellenic Data Protection Authority if the data subjects live in Greece or the alleged infringement occurred in Greece.
- **Right to basic information**
  Data subjects have the right to be provided with information relating to the processing in a concise, transparent, intelligible and easily accessible form.

## 6 Registration Formalities and Prior Approval

### 6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

Businesses are not required to register or notify the HDPA or any other governmental body in respect of their processing activities. They are, however, required to request a prior consultation with the HDPA pursuant to article 36(1) GDPR, in situations where a data protection impact assessment (DPIA) has indicated that processing activities result in a high risk which the business cannot adequately mitigate by appropriate measures. Data controllers may submit a prior consultation request to the HDPA provided that they have verified that the necessary formality criteria ensuring the completeness of the DPIA based on article 35 par. 2 and 7–9 GDPR and the Guidelines on Data Protection Impact Assessments of the European Data Protection Board (EDPB) relating to the request for consultation are met.

The request for a consultation must include at least a detailed description of the residual high risks and their potential consequences as well as a detailed documentation of the reasons for which measures to reduce the high risk to an acceptable level cannot be adopted. The request must also have the DPIA attached to it and include the elements set out in article 36(3) GDPR.

The request for prior consultation is submitted electronically, through the online portal of the HDPA and exceptionally via email.

Where the HDPA is of the opinion that the intended processing would infringe the GDPR, it shall, within a period of up to eight weeks after receiving the request, provide written advice to the controller and/or processor. That period may be extended by six weeks, taking into account the complexity of the intended processing. The time limits may be suspended until the supervisory authority has obtained the information it has requested for the purposes of the consultation.

### 6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

This is not applicable.

### 6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

This is not applicable.

### 6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

This is not applicable.

**6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?**

This is not applicable.

**6.6 What are the sanctions for failure to register/notify where required?**

This is not applicable.

**6.7 What is the fee per registration/notification (if applicable)?**

This is not applicable.

**6.8 How frequently must registrations/notifications be renewed (if applicable)?**

This is not applicable.

**6.9 Is any prior approval required from the data protection regulator?**

This is not applicable.

**6.10 Can the registration/notification be completed online?**

This is not applicable.

**6.11 Is there a publicly available list of completed registrations/notifications?**

This is not applicable.

**6.12 How long does a typical registration/notification process take?**

This is not applicable.

## 7 Appointment of a Data Protection Officer

**7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.**

The appointment of a Data Protection Officer (DPO) for controllers or processors is mandatory where: (i) the processing is carried out by a public authority or body; (ii) the core activities of the controller or the processor consist of processing which requires regular and systematic large scale monitoring of data subjects; and/or (iii) the core activities of the controller or the processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences.

Businesses are free to appoint a DPO despite not being legally obliged to do so.

In situations where an organisation designates a DPO on a voluntary basis, the relevant requirements of the GDPR concerning their designation, position and tasks apply as if the designation had been mandatory.

**7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?**

In cases where the appointment of a DPO is mandatory, failure to comply may result in the imposition by the HDPA of administrative fines up to €10 million, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

**7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?**

The appointed DPO should not be dismissed or penalised by the controller or processor for performing their tasks and should report directly to the highest management level of the organisation.

**7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?**

A group of undertakings may appoint a single DPO, provided that the DPO is easily accessible from each establishment.

**7.5 Please describe any specific qualifications for the Data Protection Officer required by law.**

DPOs should: be appointed based on professional qualities; have an expert knowledge of data protection law and practices; and be able to fulfil the tasks referred to in article 39 GDPR (see question 2.6 below). It follows that the knowledge and level of skills required will vary depending on the complexity of the processing conducted by each business.

**7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?**

The DPO supports organisations in achieving and maintaining compliance with the GDPR while also acting as a mediator between the various stakeholders. The GDPR specifies that at a minimum, the DPO must: (i) inform the controller or the processor and any employees carrying out processing activities of their responsibilities under the data protection legislation; (ii) monitor the organisation's compliance with the GDPR and other EU or Greek data protection provisions and the policies adopted by the organisations themselves; (iii) provide advice concerning the DPIA and monitor its performance; (iv) cooperate with the HDPA; and (v) act as the contact point for the HDPA. It should be noted that the role of the DPO is advisory and not decisive.

**7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?**

Yes, the controller or processor must notify the HDPA of the contact details of the designated DPO. The notification is

carried out through the online portal of the HDPA or, in exceptional cases, via email.

**7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?**

The DPO does not necessarily need to be named in the public-facing privacy notice. However, the controller or the processor must publish the contact details of the DPO to ensure unhindered communication with data subjects. The contact details must also be notified to the data subject whose personal data is being processed.

## 8 Appointment of Processors

**8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?**

Yes, where processing is to be carried out on behalf of a controller, a contract or other legal act binding the processor to the controller should be in force.

**8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?**

The agreement must be in writing and must set out the subject matter, duration, nature and purpose of the processing, the categories of data subjects and the rights and obligations of the controller. Specific contractual terms shall include the provisions of article 60 of Law 4624/2019.

## 9 Marketing

**9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).**

Electronic direct marketing requires clear affirmative consent of the recipient which must be consistent with the definition of consent and any further conditions set in GDPR. In the telecommunications sector, article 11 of L. 3471/2006 (ePrivacy Directive transposition law) states that marketing by email or SMS is not permitted without the recipient's consent unless the contact details have been acquired in the context of selling similar products/services or of another similar previous transaction. However, every email or SMS must contain the identity of the addressor and a clear opt-out option.

**9.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?**

The restrictions apply only to personal data of individuals and not companies or other legal entities. However, information in relation to sole traders may constitute personal data and restrictions may also apply to marketing addressed to employees of companies in their business account emails. The restrictions of article 11 par. 7 of L. 3471/2006 (as amended by L. 4070/2012) apply also to legal entities and therefore to a B2B context.

**9.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).**

In accordance with Directive 50/2000 of the HDPA, marketing by post needs to meet certain mandatory requirements.

Article 11 of L. 3471/2006, as amended by L. 3917/2011, provides that marketing communications by telephone are generally permitted after the controller has received and checked the registers of article 11 par. 2 L. 3471/2006 and any other lists available of people declaring their consent or objection towards marketing calls, and not included in the above registers.

When making the marketing call, the controller must follow a certain process, and if the individual objects to receiving marketing calls, a clear procedure must be followed to ensure that this number will be excluded from any future marketing activities by phone.

**9.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?**

GDPR applies to organisations that are based in the EU even if the data is stored or processed outside of the EU, as well as to organisations that are not in the EU if one of the conditions set in the GDPR apply. On the contrary, L. 3471/2006 does not have formal extraterritoriality provisions.

**9.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?**

Yes, the HDPA is active, with recent examples of imposition of a monetary fine for breach of marketing by phone restrictions (non-determination of the legal basis of the processing of personal data).

**9.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?**

Yes, under the condition that the obtaining organisation is able to demonstrate that the data was obtained in compliance with the GDPR and that it can use it for advertising purposes, as well as to ensure that the list is updated and that it does not send advertising to individuals who objected to the processing of their personal data for direct marketing purposes.

The obtaining organisation must also inform data subjects, the latest at the time of the first communication, that it has collected their personal data and that it will be processing it for sending them advertisements.

**9.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?**

The GDPR and Law 4624/2019 provide the HDPA with different options in case of non-compliance with the data protection rules

such as warnings (in case of potential infringement) or reprimands, temporary or permanent ban of processing or/and fines up to €20 million (in case of infringement).

According to L. 3471/2006, the fines for breaching the above-mentioned restrictions amount from €15,000 to €1,500,000. A warning for compliance may also be issued before the imposition of a fine.

## 10 Cookies

**10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).**

The installation and use of "cookies" are regulated by paragraph 5 of article 4 of Law 3471/2006 (which transposed into Greek law the e-Privacy Directive – 2002/58/EC). Exceptions to the above obligation are the following cases: (i) the sole purpose of the cookie is carrying out the transmission of a communication over an electronic communications network; or (ii) the cookie is strictly necessary to provide an "information society service" requested by the subscriber or user, meaning that it is essential to fulfil their request. The basic principle is that the installation and use of cookies is permitted only with the user's prior consent. For consent to be valid, it should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of their personal data. The HDPA issued its Recommendations 1/2020, providing clarifications regarding the best and worst practices on cookies, especially concerning the obligation and the way of obtaining the user's consent, as well as the way and the content of the necessary information. The EU Commission intends to pass a new ePrivacy Regulation that will replace the respective national legislation in EU Member States.

**10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?**

Yes, the applicable restrictions distinguish between different types of cookies. There are two types of cookies, those which require the user's consent and those which do not. The first category includes the necessary cookies, which are considered technically necessary (a) for the identification and/or retention of content entered by the subscriber or user during a session on a website throughout the specific connection, (b) to connect the subscriber or user to services that require authentication for user security to perform the technique of load distribution (load balancing) on a link to a website, and (c) to maintain the user's choices regarding the presentation of the website. The second category of cookies includes cookies installed for online advertising, targeting, functionality and web analytics.

**10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?**

The HDPA conducted remote audits on Controllers' websites, finding a significant lack of compliance with the specific requirements of electronic data processing legislation and the GDPR regarding the management of cookies and related technologies. However, the HDPA has not yet proceeded to any enforcement action.

**10.4 What are the maximum penalties for breaches of applicable cookie restrictions?**

In case of violation of the applicable cookie restrictions, a fine of up to 20% or up to 4% of the worldwide turnover may be imposed.

## 11 Restrictions on International Data Transfers

**11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.**

Data transfers to jurisdictions not within the European Economic Area (EEA) can only take place if the transfer is made to an "Adequate Jurisdiction" (as specified by the EU Commission), the business has implemented one of the required safeguards as specified by the GDPR, or one of the derogations specified in the GDPR applies to the relevant transfer. The EDPB Guidelines (2/2018) set out that a "layered approach" should be taken with respect to the transfer mechanisms. If the transfer is not to an Adequate Jurisdiction, the data exporter should first explore the possibility of implementing one of the safeguards provided in the GDPR before relying on a derogation. Moreover, the EDPB issued Guidelines (2/2020) on articles 46(2)(a) and 46(3)(b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies.

**11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).**

When transferring personal data to a country other than an Adequate Jurisdiction, businesses must ensure that there are appropriate safeguards on the data transfer, as prescribed by the GDPR. The GDPR offers a number of options such as consent of the data subject, Standard Contractual Clauses, Binding Corporate Rules (BCR) and contracts agreed between the data exporter and data importer. Regarding the BCRs, they will always require approval from the lead supervisory data protection authority. Concerning data transfers to the USA, following the issuance of the CJEU *Schrems II* judgment, the Commission Decision 2016/1250 on the adequacy of the protection granted by the EU-US privacy shield was declared invalid and therefore any transfer of data from the EU to the USA based on the now repealed Privacy Shield is illegal. For this reason, any transfer of personal data to the USA can be carried out by applying the alternative tools provided by article 46 GDPR, subject to certain conditions, such as their prior assessment by the parties.

**11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.**

Prior approval from the HDPA is required in the following cases:

(a) *Ad hoc* contractual clauses between data importer and exporter.

(b) Administrative arrangements between public authorities or bodies, which include enforceable and substantive rights of subjects (e.g. MoUs between public authorities with respective responsibilities). The permission of the HDPA is necessary because such administrative arrangements are legally non-binding.
(c) BCRs. In this case, the draft of the BCRs must be submitted in Greek as well.

In order to obtain the HDPA's relevant permission or submit the required notification, the data exporter should complete a special form and submit it electronically, through HDPA's web portal or via email in exceptional cases.

There is no explicit provision for the time required for approval by the HDPA of the submitted applications, but in practice it takes approximately three months (e.g., HDPA Decision 2136/2019).

**11.4 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?**

The EDPB has issued (draft) Recommendations 01/2020 on supplementary measures to be implemented where appropriate, in respect of transfers made under SCCs, in light of the *Schrems II* decision. The HDPA has not issued any guidelines or recommendations pertaining to non-EU data transfers following the issuance of *Schrems II*. At the time of writing this chapter, the draft Recommendations had not yet been finalised.

**11.5 What guidance (if any) has/have the data protection authority(ies) issued in relation to the European Commission's revised Standard Contractual Clauses?**

The European Commission has issued new SCCs. The EDPB and the European Data Protection Supervisor have issued Joint Opinion 1/2021 in relation to those SCCs. The HDPA has not issued any guidelines pertaining to the European Commission's revised SCCs.

## 12 Whistle-blower Hotlines

**12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?**

Internal whistleblowing schemes are generally established in order to implement proper corporate governance principles in the daily functioning of businesses. Whistleblowing is designed as an additional mechanism for employees to report misconduct internally through a specific channel and supplements businesses' regular information and reporting channels, e.g., employee representatives, line management, quality-control personnel or internal auditors employed precisely to report such misconducts.

The WP29 has limited its Opinion 1/2006 on the application of EU data protection rules to internal whistle-blowing schemes to the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime. The scope of corporate whistle-blower hotlines, however, does not need to be limited to any particular issues. In its Opinion, WP29 recommends that the business responsible for the whistleblowing scheme should carefully assess whether it might be appropriate to limit the number of persons eligible for reporting alleged misconduct and the number of persons who may be reported through the scheme, in particular in the light of the seriousness of the alleged offences.

There is no Greek regulation according to which companies are obliged to implement whistleblowing mechanisms and similarly, no general requirement to internally disclose any misconduct incidents before external disclosures. Greek citizens are required, however, to disclose any illegal actions that come to their attention to the Public Prosecutor according to article 40 of Penal Code.

**12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?**

Anonymous reporting is not prohibited under EU data protection law; however, it raises problems as regards the essential requirement that personal data should only be collected fairly. In Opinion 1/2006, WP29 considered that only identified reports should be advertised in order to satisfy this requirement. Businesses should not encourage or advertise the fact that anonymous reports may be made through a whistle-blower scheme.

Individuals intending to report to a whistle-blowing system should be aware that they will not suffer due to their action. Whistle-blowers, at the time of establishing first contact with the scheme, should be informed that their identity will be kept confidential at all the stages of the process, and, in particular, will not be disclosed to third parties, such as the incriminated person or to the employees' line management. If, despite this information, the person reporting to the scheme still wants to remain anonymous, the report will be accepted into the scheme. Whistle-blowers should be informed that their identity may need to be disclosed to the relevant people involved in any further investigation or subsequent judicial proceedings instigated as a result of any enquiry conducted by the whistle-blowing scheme.

The Hellenic Competition Commission very recently created a digital environment for anonymous reporting regarding illegal business practices, such as imposition of unfair prices, exclusion of competitors and products from the market, unfair commercial practices, etc. that makes anonymous reporting of illegal business practices possible.

## 13 CCTV

**13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?**

The HDPA issued on 16 October 2018 a list of the kind of processing activities, which are subject to the requirement for a DPIA. According to this list, a DPIA must be conducted by the Controllers, in cases of large-scale systematic processing for monitoring, observing or controlling natural persons using data collected through video surveillance systems over a public area, publicly accessible area or private area accessible to an unlimited number of persons. If the DPIA demonstrates that the residual risks remain high, the Controllers must consult the HDPA (see question 6.1). Regarding the required public notice in case of operation of a CCTV, the HDPA has issued its 2/2020 Recommendations, which include models for the satisfaction of the right to information when processing data through video surveillance systems. Specifically, there are provisions concerning the content of the warning signs and its accompanied privacy notices, as well as the space where they must be placed in order in any case to ensure that they are visible from all possible entry points into the monitored area.

**13.2 Are there limits on the purposes for which CCTV data may be used?**

In Directive 1/2011, the HDPA provides guidelines for the legal use of video surveillance systems in private areas accessible to the public. Based on this, the use of CCTV is permitted in order to protect persons and goods located in the monitored area or the provision of health services when the Controller is a health provider, such as hospitals or psychiatric institutions. This purpose of processing personal data is justified by the legal interest or legal obligation of the site's administrator to protect persons and property from unlawful acts. Also, according to HDPA Decision 115/2001, CCTV should not be used to monitor employees within working areas, apart from special exceptional cases where this is justified by the nature and the working conditions and is necessary to protect the health and safety of employees or critical workplaces.

The HDPA, following the issuance of Presidential Decree 75/2020 on the use of CCTV and audio recording in public spaces for the purpose of preventing and suppressing specific criminal acts, regulating traffic, and preventing and managing road accidents, published its 3/2020 Opinion, making clear its opposition to several provisions.

## 14 Employee Monitoring

**14.1 What types of employee monitoring are permitted (if any), and in what circumstances?**

Monitoring of employees could take place via monitoring of their computer resources. Employers should demonstrate that such processing is necessary and proportionate in order to pursue their legitimate interests. A clear policy is required, informing employees on whether use of computer resources for personal reasons is permitted or not and clarifying if any monitoring takes place and the purposes of such monitoring. (See HDPA's Decision 43/2019 and 44/2019). In general, as pointed out in the HDPA Decision No 34/2018 and at the *Bărbulescu v Romania Case* by ECHR, the difference between constant monitoring of an employee, in contrast to a specific and targeted investigation, for instance due to suspicion of illegal conduct, is critical when evaluating the legitimacy of an employer's monitoring actions.

Furthermore, regarding installation of CCTV systems in the workplace, article 27(7) of Law 4624/2019 specifies such a provision. Specifically, whether publicly accessible or not operation of CCTV systems shall only be permitted if it is necessary for the protection of persons and goods. However, it is clearly stated that data collected through these systems cannot be used as a criterion for evaluating the performance of employees. The employees shall be informed in writing or electronically of the installation and operation of a CCTV system in the workplace.

**14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.**

An employee's consent should not be used as a legal basis for monitoring, considering that such consent is highly unlikely to meet the criteria of being freely given, due to the unequal nature of the employment relationship. This was emphasised in the 115/2001 Guidelines of the Hellenic DPA and has been confirmed in numerous Decisions. Notification is required, in accordance with article 12 of Directive 1/2011 of the HDPA.

**14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?**

Where Work Councils exist, according to article 13 of Law 1767/1988, employers must inform the Works Council before the implementation of a decision regarding, among others, the introduction of new technology.

## 15 Data Security and Data Breach

**15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?**

Yes. Personal data must be processed through technical and organisational measures meeting the requirements of the GDPR, in a way that ensures security and safeguards against unlawful processing. This obligation applies to both controllers and processors.

**15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

In the case of a personal data breach, the controller shall without undue delay, not later than 72 hours after having become aware of it, notify the personal data breach to the HDPA, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of the natural persons. This obligation applies to the processor as well, who shall notify the controller without undue delay after becoming aware of a personal data breach. The notification must contain specific information, such as the nature/extent of the incident, the categories of persons affected, the actions taken to address and mitigate the breach, etc.

**15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay, in accordance with article 34 of the GDPR. According to article 33(5) of Law 4624/2019, the above obligation shall not apply to the extent that the notification would entail the disclosure of information which, according to the law or by reason of its nature, in particular, due to overriding legitimate interests of third parties, should remain confidential.

**15.4 What are the maximum penalties for data security breaches?**

See question 16(1)(d).

## 16 Enforcement and Sanctions

**16.1 Describe the enforcement powers of the data protection authority(ies).**

(a) **Investigative Powers**: The HDPA conducts investigations and audits on compliance with the data protection legislation, requesting and receiving all information necessary for its tasks, and access to the premises and data processing equipment. It may also carry out reviews on certificates and notify the controller/processor of alleged infringements of the legislation.

(b) **Corrective Powers**: The HDPA issues warnings or reprimands for non-compliance, setting the manner or deadline to comply, such as rectification or erasure of personal data, destruction of filing systems, disclosure of data breaches to the subjects, limitation or ban on processing, withdrawal of certifications. It may also impose administrative fines.

(c) **Authorisation and Advisory Powers**: The HDPA has the power to advise the controller, issue opinions, guidelines and recommendations, approve codes of conduct or certification criteria, issue certificates, accredit certification bodies, authorise standard and contractual clauses, administrative arrangements and binding corporate rules. The HDPA also advises data subjects, issues standard documents and complaint forms, adopts regulatory acts for specific, technical and detailed matters.

(d) **Imposition of administrative fines for infringements of specified GDPR provisions**: The HDPA may impose fines up to €10,000,000 or 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher, or, for serious violations related to data subjects' rights, fines up to €20,000,000 or 4% of the total worldwide annual turnover, whichever is higher. When the processor is a public body, the fine may be up to €10,000,000.

(e) **Non-compliance with a data protection authority**: The fines may be up to €20,000,000 or 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher. If the processor is a public body, the fine may be up to €10,000,000.

**16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?**

The HDPA has the power to impose a temporary or definitive limitation including a ban on processing.

**16.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.**

The HDPA generally examines requests and holds hearings imposing sanctions, based on the gravity and the duration of the breach, the conduct and history of the controller and the risk of repetition. In 2020–2021, the HDPA issued numerous decisions on unlawful processing in the context of political communication, imposing reprimands and fines of €1,000–€4,000. A fine of €20,000 was imposed for unlawful commercial communication and violation of the right to erasure (dec.13/2021). Fines were also imposed for CCTV in workspace (€2,000, dec.12/2021), and in residence (€8,000, dec.30/2020). Dec.11/2021 imposed on a company the obligation to modify its data erasing system within six months.

The HDPA frequently issues opinions on draft laws (e.g., Opinion 5/2020 on a draft law of the Ministry of National Defence, Opinion 3/2020 on the draft Presidential Decree on using surveillance systems in public places).

The HDPA, by Dec.9/2020, which was later modified, decided to draw up a plan outlining the requirements for the accreditation of monitoring bodies.

**16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?**

The HDPA may exercise its powers against businesses established in other jurisdictions when one processes personal data in Greek territory, or in the context of activities of a unit in Greek territory.

## 17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

**17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?**

E-discovery and disclosure requests are not part of the Greek legal framework. Such requests are assessed by businesses depending on their legal basis, their purpose and on the nature and type of information requested.

**17.2 What guidance has/have the data protection authority(ies) issued?**

The HDPA has not issued relevant guidance.

## 18 Trends and Developments

**18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.**

During the previous 12 months, the HDPA issued 27 decisions on unlawful data processing for the purpose of political communication. The HDPA imposed reprimands and fines ranging from €1,000 to €4,000 for not requesting political communication by electronic means or post. The HDPA took into consideration the general conduct and history of the controller, how the data had been collected, whether the controller had implemented an opt-out system, and whether the right to erasure had been exercised.

**18.2 What "hot topics" are currently a focus for the data protection regulator?**

As it would be expected, this year the HDPA has been concerned with data protection issues arising from the COVID-19 situation, issuing Guidelines 1/2020 on Data Processing in the context of management of COVID-19, Guidelines 2/2020 on the adoption of security measures in the context of teleworking and Opinion 4/2020 on distance learning in primary and secondary education.

**Dr. Nikos Th. Nikolinakos** is the Managing Partner of Nikolinakos & Partners LLP and co-head of the TMT, Digital Business and Competition Law practices. He features prominently in the TMT, data protection/cybersecurity, competition law and IP rankings of leading bar publications such as *Chambers and Partners* and *The Legal 500*.
Nikos divides his specialised practice between regulatory and policy advice in the TMT sector, and in EU/national competition law, data protection and cybersecurity, emerging digital technologies (such as AI and IoT), IP rights advocacy and compliance. Prior to founding the firm, Nikos held the post of general counsel – legal and regulatory affairs director for a major telecoms operator and internet provider in Greece. He also held the position of senior in-house adviser to the Telecommunications & Post Commission of Greece (EETT), responsible for competition law and regulatory policy/compliance. He has filled senior consulting roles in various international projects for governments, national regulatory authorities, market players and the European Commission.
Nikos has been a Visiting Lecturer on electronic communications law, data protection/cybersecurity, competition law and intellectual property at the AIT Center and at NTUA (the National Technical University of Athens). Nikos is the author of numerous contributions in books and refereed journals in the fields of TMT, new technologies and competition law. He is also the author of *EU Competition Law and Regulation in the Converging Telecommunications, Media & IT Sectors* (2006, Kluwer Law International/Aspen Publishers).
Education: National University of Athens, School of Law (LL.B.); and the University of Edinburgh, School of Law (LL.M. and Ph.D.).

**Nikolinakos & Partners Law Firm**
182, Mesogeion Avenue
P.C.15561, Athens
Greece

Tel: +30 2130 020 020
Email: nikolinakos@nllaw.gr
URL: www.nllaw.gr

**Dina Th. Kouvelou** is a Partner, head of the Data Protection & Cybersecurity practice and co-head of the TMT and Digital Business practice of Nikolinakos & Partners LLP. Dina is recommended as a leading TMT, data privacy and competition legal counsel by *Chambers and Partners* ("a true TMT expert", "a competition law expert who is extremely business oriented, proactive, and an effective strategist") and *The Legal 500* ("an outstanding regulatory counsel" who "provides a hard-to-find combination of technical and practical legal advice").
During the last 20 years, Dina's professional career has spanned TMT, data protection, betting and gaming, competition law and corporate/commercial law experience in, amongst others, the following roles: general counsel and head of legal & regulatory affairs in a leading alternative fixed telecoms operator and in a mobile operator in Greece; senior competition law and regulatory policy advisor in the Legal Department of the National Regulatory Authority (EETT); and legal consultant in regulatory, competition law and commercial law projects with Greek and international law firms and consultancies.
Education: National University of Athens, School of Law; University College of London – Queen Mary (LL.M., computer and communications law).

**Nikolinakos & Partners Law Firm**
182, Mesogeion Avenue
P.C.15561, Athens
Greece

Tel: +30 2130 020 020
Email: kouvelou@nllaw.gr
URL: www.nllaw.gr

**Alexis N. Spyropoulos** is a Partner, head of the Administrative Law & Public Procurement Practice of Nikolinakos & Partners LLP. He acted from 2007 to 2015 as Head of the Legal Department of the Hellenic Telecommunications & Postal Regulatory Commission (EETT) handling numerous complaints, actions, and infringement proceedings.
Alexis is experienced in representing undertakings and Government bodies in all kinds of proceedings (including competition law and data protection issues) before administrative courts and regulatory authorities (such as the DPA – Data Protection Authority of Greece). He has extensive (20 years) experience in the fields of TMT, Administrative Law, Data Protection & Administrative Law.
Education: National University of Athens, School of Law; University of Sheffield, LL.M. in Commercial Law, Intellectual Property Law, Insurance Law & Competition Law.

**Nikolinakos & Partners Law Firm**
182, Mesogeion Avenue
P.C.15561, Athens
Greece

Tel: +30 2130 020 020
Email: spyropoulos@nllaw.gr
URL: www.nllaw.gr

# India


Harsh Walia


Supratim Chakraborty

Khaitan & Co LLP

## 1 Relevant Legislation and Competent Authorities

### 1.1 What is the principal data protection legislation?

Currently, India does not have comprehensive and dedicated data protection legislation. Some provisions of the Information Technology Act, 2000, as amended from time to time ("**IT Act**") and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("**SPDI Rules**") framed under it deal with protection of personal information ("**PI**") and sensitive personal data and information ("**SPDI**").

There has been considerable traction with regard to data protection in recent times. The Government recently presented the Personal Data Protection Bill, 2019 ("**PDP Bill**") in Parliament and it is currently pending consideration before a Joint Parliamentary Committee. Although the PDP Bill has not been enacted, it is expected that it will soon see the light of day; we have therefore also touched upon its provisions as part of our responses to the questions below (on the assumption that it will be enacted in its present form), for the sake of completeness.

### 1.2 Is there any other general legislation that impacts data protection?

Please refer to our response to question 1.1 above.

### 1.3 Is there any sector-specific legislation that impacts data protection?

There is no sector-specific legislation; however, there are regulations, directives and licence conditions issued by sectoral regulators in relation to payment systems, telecoms, healthcare, e-pharmacies, etc., that stipulate certain data protection obligations.

### 1.4 What authority(ies) are responsible for data protection?

At present, there is no dedicated authority responsible for data protection in India. The IT Act contemplates the appointment of Adjudicating Officers for adjudicating whether provisions of the IT Act have been contravened. However, the implementation of this mechanism on the ground with regard to data protection has been fairly bleak. The PDP Bill envisages the constitution of the Data Protection Authority of India ("**DPAI**") for enforcement of its provisions.

## 2 Definitions

### 2.1 Please provide the key definitions used in the relevant legislation:

- "**Personal Data**"
  The SPDI Rules define "personal information" as "*any information that relates to a natural person which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person*".
  The PDP Bill defines "personal data" as "*data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling*".
- "**Processing**"
  The IT Act and SPDI Rules do not define the term "processing". However, the PDP Bill defines "processing", in relation to personal data, as "*an operation or set of operations performed on personal data, and may include operations such as collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, use, alignment or combination, indexing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction*".
- "**Controller**"
  The IT Act and SPDI Rules do not define the term "controller". However, the PDP Bill defines the term "data fiduciary", which is akin to a data controller, as "*any person, including the State, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data*".
- "**Processor**"
  The IT Act and SPDI Rules do not define the term "processor". However, the PDP Bill defines a "data processor" as "*any person, including the State, a company, any juristic entity or any individual, who processes personal data on behalf of a data fiduciary*".
- "**Data Subject**"
  The IT Act and SPDI Rules do not define the term "data subject". However, the PDP Bill defines "data principal", akin to a data subject, as "*the natural person to whom the personal data relates*".
- "**Sensitive Personal Data**"
  The SPDI Rules define SPDI to mean:
  "*Any such personal information which consists of information relating to:*

i. *Password;*
ii. *Financial information such as bank account or credit card or debit card or other payment instrument details;*
iii. *Physical, physiological and mental health condition;*
iv. *Sexual orientation;*
v. *Medical records and history;*
vi. *Biometric information;*
vii. *Any detail relating to the above clauses as provided to controller for providing service; and*
viii. *Any of the information received under above clauses by controller for processing, stored or processed under lawful contract or otherwise.*

*Provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of SPDI Rules.*"

The PDP Bill widens and amends the definition of "sensitive personal data" to include certain additional categories such as: transgender status; intersex status; caste or tribe; and religious or political belief or affiliation. However, "password" has been excluded from the definition.

- "**Data Breach**"
  The IT Act and the rules made thereunder do not define the term "data breach". However, under the Indian Computer Emergency Response Team and Manner of Performing Functions and Duties Rules 2013, "cyber security incidents" have been defined to mean "*any real or suspected adverse event in relation to cyber security that violates an explicitly or implicitly applicable security policy resulting in unauthorized access, denial of service or disruption, unauthorized use of a computer resource for processing or storage of information or changes to data, information without authorisation*".
  The PDP Bill defines "personal data breach" as "*any unauthorised or accidental disclosure, acquisition, sharing, use, alteration, destruction of or loss of access to, personal data that compromises the confidentiality, integrity or availability of personal data to a data principal*".
- **Other key definitions**
  The PDP Bill defines "anonymised data" as "*data which has undergone the process of anonymisation*". In this regard, "anonymisation" in relation to personal data, has been defined to mean such "*irreversible process of transforming or converting personal data to a form in which a data principal cannot be identified, which meets the standards of irreversibility specified by*" the Data Protection Authority.

## 3 Territorial Scope

### 3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The question of applicability of the IT Act and SPDI Rules on an entity incorporated outside India is not a very straightforward one and remains a grey area. However, the IT Act has extra-territorial operation and applies "*to any offence or contravention committed outside India by any person irrespective of his nationality*", as long as the act constituting the offence or contravention involves a "*computer*" or "*computer system*" in India.

Moreover, the SPDI Rules cast obligations on "bodies corporate" that process SPDI, and the definition of "*body corporate*" under the IT Act does not restrict this to entities incorporated within India only.

The provisions of the PDP Bill are slightly clearer on this aspect. According to the PDP Bill, its provisions will be applicable to the processing of personal data by data fiduciaries and data processors not present in India if such processing is in connection with: any business carried out in India; any systematic activity of offering goods and services to data principals within India; or any activity which involves the profiling of data principals within India.

## 4 Key Principles

### 4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  According to the SPDI Rules, collecting entities are required to ensure that a provider of SPDI has knowledge of: the fact that SPDI is being collected; the purpose of collection of SPDI; the intended recipients of SPDI; and the name and address of the agency collecting and retaining SPDI. Further, before the disclosure of a data subject to any third party, the consent of such person is required to be obtained, unless the data subject has already agreed to such disclosure in the contract pursuant to which SPDI was provided, or such disclosure is necessary for compliance with a legal obligation.
- **Lawful basis for processing**
  Under the SPDI Rules, consent is required to be obtained for collecting and processing SPDI.
  The PDP Bill provides for certain bases on which collecting entities can rely to process personal data, such as: consent having been given; employment purposes; and reasonable purposes to be notified by the DPAI, etc. Bases for processing sensitive personal data include explicit consent, among others.
- **Purpose limitation**
  The SPDI Rules provide that SPDI should only be collected for a lawful purpose connected with a function or activity of the body corporate or any person acting on its behalf.
  The PDP Bill requires the processing of personal data to be done in a fair and reasonable manner, ensuring the privacy of the data principal, and for the purpose consented to by the data principal or which is incidental to or connected with such purpose, for which the data principal would reasonably expect that such personal data would be used, and in the context and circumstances in which the personal data was collected.
- **Data minimisation**
  While there is no express principle of data minimisation, the SPDI Rules provide that collection of SPDI is permitted only if it is considered necessary for that purpose.
  The PDP Bill states that personal data should be collected only to the extent that is necessary for the purposes of processing such personal data.
- **Proportionality**
  There is no such express principle under the IT Act and SPDI Rules.
  Please see our response under "Purpose limitation" above with respect to the PDP Bill.
- **Retention**
  The SPDI Rules provide that SPDI is not permitted to be retained for longer than is required for the purposes for which the SPDI may lawfully be used or is otherwise required under any other law for the time being in force.

The PDP Bill mandates that a data fiduciary should not retain any personal data beyond the period necessary to satisfy the purpose for which it is processed and shall delete the personal data at the end of the processing.

- **Accountability**
  There is no such express principle under the IT Act and SPDI Rules.
  The PDP Bill provides that a data fiduciary will be responsible for complying with the provisions of the PDP Bill in respect of any processing undertaken by it or on its behalf.

## 5 Individual Rights

### 5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**
  Providers of SPDI have the right at any time to request a review of SPDI provided by them to collecting entities under the SPDI Rules.
  The PDP Bill proposes a similar right where a data principal can obtain (i.e. access) personal data (or a summary thereof) from the data fiduciary by making a written request (directly or through consent managers), and stipulates that such requests must be fulfilled in a timely manner.
- **Right to rectification of errors**
  Providers of SPDI have a right to seek corrections or amendments to their SPDI in respect of any inaccuracies or deficiencies under the SPDI Rules.
  In this regard, a similar right of rectification has been proposed under the PDP Bill along with related modalities (such as the circumstances in which rectification requests may be refused by data fiduciaries, and the procedure to be adopted pursuant to such refusals).
- **Right to deletion/right to be forgotten**
  Such right has not been explicitly provided under the IT Act or SPDI Rules. However, the right to deletion of inaccurate or deficient information may be regarded as being a part of the right to correction or amendment of SPDI as described above.
  The right to be forgotten has been proposed under the PDP Bill. Under this proposed right, a data principal may restrict continued disclosure of its personal data upon obtaining a suitable direction from a proposed adjudicatory authority, in cases where: (a) disclosure of such data has served its purpose; (b) the disclosure is no longer necessary for such purpose; (c) the data principal has withdrawn its consent to such disclosure; or (d) such disclosure was contrary to the provisions of the PDP Bill or any other applicable law.
- **Right to object to processing**
  No such right has been explicitly provided under the IT Act and SPDI Rules or proposed under the PDP Bill.
- **Right to restrict processing**
  No such right has been explicitly provided under the IT Act and SPDI Rules or proposed under the PDP Bill.
- **Right to data portability**
  No such right has been explicitly provided under the IT Act and SPDI Rules.
  Such a right has been proposed under the PDP Bill in the context of data processing undertaken through automated means. In such cases, a data principal has a right to receive certain information relating to their personal data from a data fiduciary in a structured and machine-readable format. Further, data principals may require data fiduciaries to transfer such data to another data fiduciary.
- **Right to withdraw consent**
  Providers of SPDI have the option to withdraw consent given to a body corporate at any time while availing themselves of its services, by giving notice in writing under the SPDI Rules. In such cases, the body corporate has the option of not providing the goods or services for which such information was sought.
  Similar rights have also been proposed under the PDP Bill, where it is specified that consent to processing provided by a data principal must be capable of being withdrawn.
- **Right to object to marketing**
  Providers of SPDI have the option to withdraw consent given to a body corporate at any time while availing themselves of its services, by giving notice in writing under the SPDI Rules. In such cases, the body corporate has the option of not providing the goods or services for which such information was sought.
  Similar rights have also been proposed under the PDP Bill, where it is specified that consent to processing provided by a data principal must be capable of being withdrawn.
- **Right to complain to the relevant data protection authority(ies)**
  As noted in our response to question 1.4 above, there is no dedicated data protection authority at present. Providers of SPDI may register their grievances with respect to the processing of SPDI with the "Grievance Officers" of the collecting entities appointed under the SPDI Rules. Also, complaints regarding the payment of compensation *in lieu* of failure to protect SPDI may be raised by aggrieved persons before the adjudicating officer appointed under the IT Act. Further criminal proceedings in respect of unlawful disclosure of SPDI may be instituted with police authorities. Cyber security incidents relating to unauthorised access to IT systems/data and compromise of information may also be reported by affected individuals or organisations to the Computer Emergency Response Team – India ("**CERT-IN**").
  The PDP Bill proposes that complaints in relation to contravention of the Bill's provisions be made by a data principal to the data fiduciary's designated grievance redressal officer. Such complaints may also be made to the DPAI.
- **Other key rights**
  Under the IT Act and SPDI Rules, it must be ensured by the collector that the provider of SPDI has knowledge about the fact that information is being collected, the purpose for which it is being collected, the intended recipients of the information, and names and addresses of the agency that is collecting and will retain the information.

## 6 Registration Formalities and Prior Approval

### 6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

There is no such requirement under the IT Act and rules thereunder.

Under the PDP Bill, the DPAI (and by the Central Government in consultation with the DPAI, in the case of social media intermediaries) may notify any data fiduciary, class of data fiduciary

or certain social media intermediaries, as a significant data fiduciary ("**SDF**"), based on certain factors provided under the PDP Bill. Such SDF is required to register itself with the DPAI in such manner as may be specified by regulations. We have provided responses to questions 6.2 to 6.12 below from this perspective.

**6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?**

Under the PDP Bill, the DPAI may notify a data fiduciary or class of data fiduciary as an SDF with regard to the following factors:

(a) volume of personal data processed;
(b) sensitivity of personal data processed;
(c) turnover of the data fiduciary;
(d) risk of harm posed by processing undertaken by the data fiduciary;
(e) use of new technologies for processing; and
(f) any other factor causing harm from such processing.

Additionally, if the DPAI is of the opinion that any processing by any data fiduciary or class of data fiduciary carries a risk of significant harm to any data principal, it may, by notification, apply all or any of the obligations of an SDF to such data fiduciary or class of data fiduciary as if it were an SDF.

Further, the Central Government, in consultation with the DPAI, may notify a social media intermediary as an SDF, if such social media intermediary has users: (i) above such threshold as may be notified by the Central Government, in consultation with the DPAI; and (ii) whose actions have, or are likely to have, a significant impact on electoral democracy, security of the State, public order or the sovereignty and integrity of India.

**6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?**

Please see our response to question 6.2 above.

**6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?**

Please see our response to question 6.1 above.

**6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?**

The PDP Bill is yet to come into force and regulations in this regard are yet to be released.

**6.6 What are the sanctions for failure to register/notify where required?**

Under the PDP Bill, failure to register as an SDF, if so required, shall be liable to a penalty that may extend to INR 5 crores (approx. USD 6.87 million) or 2 per cent of its annual worldwide turnover of the preceding financial year, whichever is higher.

**6.7 What is the fee per registration/notification (if applicable)?**

Please see our response to question 6.5 above.

**6.8 How frequently must registrations/notifications be renewed (if applicable)?**

Please see our response to question 6.5 above.

**6.9 Is any prior approval required from the data protection regulator?**

This is not applicable.

**6.10 Can the registration/notification be completed online?**

Please see our response to question 6.5 above.

**6.11 Is there a publicly available list of completed registrations/notifications?**

This is not applicable.

**6.12 How long does a typical registration/notification process take?**

Please see our response to question 6.5 above.

## 7 Appointment of a Data Protection Officer

**7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.**

The current legal framework relating to data protection does not contemplate the appointment of a Data Protection Officer ("**DPO**"). Having said that, the SPDI Rules speak of the appointment of a Grievance Officer to redress the grievances of the provider of SPDI with respect to the processing of her/his SPDI in a timely manner. All entities that process SPDI of natural persons in India are required to comply with this requirement.

The PDP Bill envisages mandatory appointment of a DPO by SDFs only.

**7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?**

Under the current legal framework, there is no sanction or penalty *per se* for failing to appoint a Grievance Officer. However, appointment of a Grievance Officer is a step towards demonstrating compliance with reasonable security practices and procedures contemplated under the IT Act and SPDI Rules. In the case that an entity is negligent in adhering to reasonable security practices and procedures, it may be exposed to a claim for compensation if the Provider has suffered a "wrongful loss".

With respect to the PDP Bill, in the case that an SDF fails to appoint a DPO, it shall be liable to a penalty of up to INR 5 crores (approx. USD 6.75 million) or 2 per cent of its annual

worldwide turnover of the preceding financial year, whichever is higher. Additionally, a claim for compensation can be made by an affected data principal.

**7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?**

There are no specific exemptions of this nature under the current law or under the PDP Bill.

**7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?**

Neither the current legal framework nor the PDP Bill set out any restriction on appointment of a single Grievance Officer/DPO to cover multiple entities. From a practical standpoint, this practice appears to be fairly commonplace.

**7.5 Please describe any specific qualifications for the Data Protection Officer required by law.**

The IT Act and SPDI Rules do not set forth any specific qualifications of the Grievance Officer. Under the PDP Bill, regulations setting out qualifications and experience of the DPO can be framed.

**7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?**

Under the IT Act and SPDI Rules, the Grievance Officer is required to provide redressal to grievances of providers of SPDI expeditiously, within a maximum of 30 days.

The DPO under the PDP Bill has multiple functions, e.g. providing information and advice to SDFs on compliance with provisions, monitoring processing activities, providing advice on the carrying out of Data Privacy Impact Assessments, providing advice on the development of internal systems to enable rights of data principals, providing assistance to and cooperating with the DPAI, etc.

**7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?**

There is no such requirement under the current law or even under the PDP Bill.

**7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?**

According to the SPDI Rules, the name and contact details of the Grievance Officer are required to be published. Similar obligations exist under the PDP Bill in respect of DPOs.

## 8 Appointment of Processors

**8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?**

The IT Act and rules thereunder do not provide for such a requirement.

Under the PDP Bill, a data fiduciary is not permitted to engage, appoint, use or involve a data processor to process personal data on its behalf without a contract entered into by the data fiduciary and such data processor.

**8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?**

The PDP Bill does not specify the exact matters that are to be spelt out in the contract. While not expressly stated, it is recommended that the contract is in written form.

## 9 Marketing

**9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).**

The regulatory regime relating to delivery of, *inter alia*, marketing or "promotional" messages/calls to customers in India is currently encapsulated under the Telecom Commercial Communications Customer Preference Regulations, 2018, as amended ("**TCPR 2018**"), issued by the Telecom Regulatory Authority of India ("**TRAI**"). According to TCPR 2018, certain conditions are required to be met before sending any promotional communication. *Inter alia*, it must be ensured that the promotional messages are (a) in line with the category of preference (e.g. real estate, hospitality, food and beverage, etc.) indicated by the recipient, and (b) sent with the prior consent of the recipient. The modalities are prescribed by the telecom service provider ("**TSP**") under their respective "Codes of Practice". Additionally, entities engaged in sending promotional messages are, *inter alia*, required to register themselves and the message template against specific registered headers with TSPs prior to sending such promotional messages.

Notably, TCPR 2018 only deals with commercial communications sent over telecom services provided by a licensed TSP in India (e.g. SMS and phone calls). As such, TCPR 2018 does not apply to promotional messages sent over email.

**9.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?**

No. As far as the requirements for sending/making promotional communication are concerned, TCPR 2018 does not distinguish between B2C and B2B purposes.

**9.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).**

In the interest of brevity, please refer to our response to question 9.1 above. Since TCPR 2018 is only applicable in respect of promotional messages sent/made over telecom services provided by a TSP, marketing carried out by post is not covered under TCPR 2018.

**9.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?**

TCPR 2018 is mainly applicable in case of commercial communications sent from senders and telemarketers within India to recipients in India. However, TCPR 2018 provides that the TRAI may issue directions to control bulk international messages. No such directions have been issued thus far under TCPR 2018.

**9.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?**

Matters relating to breach of TCPR 2018 are largely governed by the agreement between the sender/telemarketer and TSP, and thereafter between the TSP and TRAI. Since TCPR 2018 is relatively new, the stakeholders in the ecosystem are still calibrating their processes; however, enforcement is expected to improve in the near future.

**9.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?**

The law with regard to the purchasing of marketing lists from third parties is currently a grey area; however, on the ground, such practices are fairly common. To mitigate exposure, it is advisable to seek appropriate representations and warranties from the third parties who provide such lists, stating that information set forth in such lists is collected with the consent of the persons concerned. Further, before sending/making any promotional communication, it is important to undertake the steps outlined in our response to question 9.1 above.

**9.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?**

TCPR 2018 provides a multi-pronged penalty structure, including the imposition of caps on usage of telecom resources, and a tier-wise monetary penalty scheme, depending on factors such as frequency of offences, status of the telemarketer (whether they are registered or not), etc.

## 10 Cookies

**10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).**

The IT Act and rules thereunder do not provide for any express restriction regarding cookies. However, please note that under section 43 of the IT Act, any person who, without permission from the owner of a computer, *inter alia*, downloads, copies or extracts any data or information from such computer, may be liable to pay damages by way of compensation to the person so affected.

It is important to note that data under the IT Act has been defined very widely and means a representation of information, knowledge, facts, concepts or instructions, etc.

In light of section 43 of the IT Act and the definitions provided hereinabove, it may be construed that permission from the owner or any other person who is in charge of a computer may be required to be obtained before installing cookies or similar technology on such systems. However, there is no official guidance or judicial precedent in this regard.

**10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?**

No such distinction is made.

**10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?**

No; as stated above, there is no specific provision related to cookies under the IT Act and rules thereunder.

**10.4 What are the maximum penalties for breaches of applicable cookie restrictions?**

As stated above, there is no specific provision related to cookies under the IT Act and rules thereunder.

## 11 Restrictions on International Data Transfers

**11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.**

According to the SPDI Rules, SPDI may be transferred by the collecting entity to an entity in another jurisdiction provided that the transferee entity ensures the same level of data protection that is adhered to by the transferor under the SPDI Rules. Further, the transfer is allowed only if it is necessary for the performance of a lawful contract or where the provider of SPDI has consented to such data transfer.

The PDP Bill proposes that SPD (this refers to sensitive personal data under clause 3(36) of the PDP Bill) may be transferred outside India, if explicit consent is provided by the data principal and such transfer is pursuant to an approved intra-group scheme or has been approved by the Central Government or DPAI. SPD transferred in the above manner must continue to be stored in India. CPD (this refers to "critical personal data" as defined under clause 33(2) of PDP Bill) may only be processed in India.

**11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).**

Businesses typically obtain prior consent of data subjects (such as in contracts executed with data subjects) before undertaking cross-border data transfer of SPDI. Further legal, technical and security audits of information systems may also be commissioned by businesses to ensure due adherence to the applicable Indian and foreign requirements in relation to data protection.

**11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.**

No such requirements are prescribed under the IT Act or SPDI Rules.

Under the PDP Bill, transfers of SPD outside India may require approval from DPAI or the Central Government.

**11.4 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?**

At present, there is no dedicated authority responsible for data protection in India. Even otherwise, no specific guidance has been issued by the Indian Government following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18).

**11.5 What guidance (if any) has/have the data protection authority(ies) issued in relation to the European Commission's revised Standard Contractual Clauses?**

At present, there is no dedicated authority responsible for data protection in India. No specific guidance has been issued by the Government of India in relation to the European Commission's revised Standard Contractual Clauses.

## 12 Whistle-blower Hotlines

**12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?**

All listed companies and certain other classes of companies are required to establish a vigil (whistle-blowing) mechanism to report ethical concerns to management, under the Companies Act 2013 ("**CA 2013**") read with the Companies (Meetings of Board and its Powers) Rules 2014 ("**CA Board Rules**"). It is stipulated, under the CA 2013, that the vigil mechanism should provide for adequate safeguards against the victimisation of persons who use such mechanism, and make provision for direct access to the chairperson of the audit committee or the director nominated to play the role of audit committee (in case of companies that are not required to have an audit committee).

Also, a similar requirement is provided, under the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations 2015 ("**SEBI LODR**"), on listed entities to devise an effective whistle-blower mechanism enabling stakeholders, including individual employees and their representative bodies, to freely communicate their concerns about illegal or unethical practices. Under SEBI LODR, the vigil mechanism shall provide for adequate safeguards against victimisation of director(s) or employee(s) or any other person who avail themselves of the mechanism, and shall also provide for direct access to the chairperson of the audit committee in appropriate or exceptional cases.

**12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?**

Please refer to our response to question 12.1 above.

## 13 CCTV

**13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?**

No such requirements have been prescribed under the IT Act and SPDI Rules. Further, such requirements have also not been proposed under the PDP Bill.

**13.2 Are there limits on the purposes for which CCTV data may be used?**

No specific limitation on the purposes for which CCTV data may be used have been imposed under the IT Act or SPDI Rules, provided that such purposes are lawful. In the case that any SPDI (or personal data in the case of the PDP Bill) forms part of such CCTV data, requirements under the SPDI Rules (or as proposed under the PDP Bill) may become applicable in respect of such data.

## 14 Employee Monitoring

**14.1 What types of employee monitoring are permitted (if any), and in what circumstances?**

The IT Act and rules thereunder do not contain express provisions regarding permissibility or restrictions on the monitoring of employees. If such monitoring entails the collection of SPDI, then relevant obligations under the SPDI Rules will have to be adhered to.

**14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.**

Please refer to our response to question 14.1 above.

**14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?**

There is no specific requirement in this regard under the IT Act and SPDI Rules.

## 15 Data Security and Data Breach

**15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?**

Entities processing SPDI are required to adhere to reasonable security practices and procedures as prescribed under the SPDI Rules. This includes implementing standards such as IS/ISO/

IEC 27001 prior to processing any SPDI, and preparing and deploying information security programmes complying with the stipulated requirements.

Comparatively stricter obligations have been proposed under the PDP Bill in relation to ensuring the security of personal data. These include preparing policies relating to privacy by design, complying with data audit requirements and maintaining specified processing-related records.

**15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

Cyber security incidents involving unauthorised access to IT systems/data and the compromising of information must be reported by service providers, intermediaries, data centres and bodies corporate to CERT-IN. Such incidents are required to be reported, along with prescribed details, within a reasonable time from the occurrence or noticing of the incident, in order that there is scope for timely action.

Mandatory requirements to report data breaches to DPAI have also been proposed under the PDP Bill.

**15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

No mandatory requirement to report data breaches to affected data subjects is prescribed under the IT Act and related rules. However, authorities like CERT-IN may report such data breaches to the general public and relevant stakeholders, including for resolving and preventing cyber security incidents and cyber security breaches and for promoting awareness.

Under the PDP Bill, data fiduciaries may be required to report data breaches to the affected data subject, if the same is so directed by the DPAI.

**15.4 What are the maximum penalties for data security breaches?**

Negligent disclosure of personal information may result in a claim for compensation against the disclosing entity under the IT Act. Further unlawful disclosure of personal information with criminal intent is punishable with imprisonment for a term of up to three years or a fine of up to INR 5 lakhs (approx. USD 6,700).

For such cases, penalties up to an amount being the higher of INR 15 crores (approx. USD 2 million) or 4 per cent of the total worldwide turnover of a data fiduciary have been proposed under the PDP Bill.

## 16 Enforcement and Sanctions

**16.1 Describe the enforcement powers of the data protection authority(ies).**

(a) **Investigative Powers**: Police officers not below the rank of inspector are authorised to investigate offences under the IT Act.

(b) **Corrective Powers**: Please refer to our response to question 16.1 (e) below.

(c) **Authorisation and Advisory Powers**: Please refer to our response to question 16.1 (e) below.

(d) **Imposition of administrative fines for infringements of specified GDPR provisions**: Please refer to our response to question 16.1 (e) below.

(e) **Non-compliance with a data protection authority**: There is no concept of a data protection authority (or any other similar dedicated authority) under the IT Act and rules thereunder. In this regard, please note that for the purpose of adjudicating any offence committed under the IT Act, the Central Government of India has appointed adjudicating officers. The adjudicating officers can adjudicate matters in which the claim for injury or damage does not exceed INR 5 crores. Such adjudicating officer has been given some powers of a civil court and any other matter as may be prescribed.

Jurisdiction in respect of claims for injury or damage exceeding INR 5 crores vests with the competent court. The Telecom Disputes Settlement and Appellate Tribunal ("**TDSAT**") has been notified by the Central Government as the competent appellate tribunal under the IT Act.

**16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?**

Under section 69-A of the IT Act read with the Information Technology (Procedure & Safeguards for Blocking for Access of Information by Public) Rules 2009, either the Central Government, through its designated officers, or competent courts, through orders, may direct any agency of Government or any intermediary to block access by the public to information in the interests of the sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order, or of preventing incitement to the commission of any cognisable offence related to the above.

**16.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.**

There is very selective enforcement of the IT Act. Judicial precedents are minimal and scattered in nature and, generally, token fines have been levied. In one case, a bank had authorised a transfer of funds to a different account and disclosed certain account information having received authorisation from a third-party email, whereas the actual account holder (complainant) had not opted for email authorisation. The adjudicating officer had held that for determining liability under the IT Act, negligence in authorising wrongful fund transfer was not required to be proven, but instead the negligence in implementing and maintaining reasonable security practices and procedures leading to wrongful loss to the claimant was to be proven. The adjudicating officer held that disclosing account information (which is SPDI) to a third party had caused wrongful loss to the complainant.

**16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?**

Please note that by virtue of section 75 (1) of the IT Act,

extra-territorial jurisdiction is accorded to the adjudicating officer for offences or contraventions of the IT Act committed outside India by any person, irrespective of nationality. Sub-section (2) of section 75 of the IT Act caveats the applicability by stating that the act or conduct constituting such offence or contravention should involve a computer, computer system or computer network located in India. However, we have not seen this power being exercised so far by adjudicating officers.

## 17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

### 17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Broadly speaking, businesses are not obligated to respond to any foreign e-discovery or disclosure requests unless there is a specific court order or the request is made pursuant to the "mutual legal assistance treaty" framework.

### 17.2 What guidance has/have the data protection authority(ies) issued?

No guidance has been issued on this aspect to date.

## 18 Trends and Developments

### 18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

Please refer to our response to question 16.3 above.

### 18.2 What "hot topics" are currently a focus for the data protection regulator?

As mentioned under question 1.4 above, the IT Act and rules thereunder do not provide for a data protection regulator.

**Harsh Walia** is a partner in the New Delhi office of the firm. He is a leading lawyer in the field of data protection, technology and telecommunications. Harsh has been ranked as "*Next Generation Partner*" for TMT and "*Recommended Lawyer*" for data protection by *The Legal 500 2021* Asia Pacific rankings. He has also been recognised by the *India Business Law Journal* in the Indian Law Firm Awards. He has featured in the 2020 *Business World 40 Under 40* elite list of lawyers and legal influencers in India.
He has advised various foreign-based and Indian clients on complex matters pertaining to data privacy, outsourcing, telecommunications, cloud computing and emerging technologies.
Harsh has authored several articles pertaining to data protection and regularly engages with Government and industry bodies on upcoming laws relating to data protection.
He has also obtained an FAS certification from the GDPR Institute.

**Khaitan & Co LLP**
Max Towers, 7th & 8th Floors
Sector 16B, Noida
Gautam Buddh Nagar 201 301
India

Tel: +91 120 479 1000
Email: harsh.walia@khaitanco.com
URL: www.khaitanco.com

**Supratim Chakraborty** is a partner in the Corporate and Commercial Practice Group of Khaitan & Co. He specialises in mergers, acquisitions, joint ventures and general corporate law advisory. He also specialises in information technology laws, data privacy and cyber security. Supratim has advised several clients on white-collar crime-related issues as well. Supratim has been recognised as a Notable Practitioner in the *IFLR 1000 2020* rankings. He has also been categorised as a "*Recommended Lawyer*" in the prestigious *RSG India Report 2019*. Supratim has also been recognised as a "*Leading Individual*" in *The Legal 500 2021* edition for Data Protection in India.
Supratim is a member of ASSOCHAM's National Council for FinTech, Digital Assets and Blockchain Technology. He has spearheaded some of the important stakeholder consultation meetings/feedback sessions organised by industry associations on the draft Personal Data Protection Bill. Supratim holds GDPR FAS Certification and DPO Certification. He has spoken at eminent forums and has authored several articles for renowned publications.

**Khaitan & Co LLP**
Emerald House
1B Old Post Office Street
Kolkata 700 001
India

Tel: +91 33 2248 7000
Email: supratim.chakraborty@khaitanco.com
URL: www.khaitanco.com

Founded in 1911, Khaitan & Co is among India's oldest law firms, with its roots embedded deep in our country's history. It is also one of India's leading full-service law firms. What began with a handful of people in a small office space in Kolkata is today a firm with over 700 lawyers, including close to 172 partners and directors.
From banking to taxation, mergers to dispute resolution and even dynamic areas like data privacy and competition law, Khaitan & Co has strong capabilities across practices. Our presence is pan-Indian, with offices in Delhi, Noida, Mumbai, Bengaluru, Chennai and Kolkata. The Firm also has capabilities in overseas markets via strong working relationships with top international law firms across jurisdictions; these include full-service firms as well as those with niche practice areas. We have opened our first international office in Singapore this year.

**www.khaitanco.com**

KHAITAN &CO
Advocates since 1911

# Indonesia



Steffen Hadi


Sianti Candra


Dimas Andri Himawan

H & A Partners
in association with Anderson Mōri & Tomotsune


## 1 Relevant Legislation and Competent Authorities

### 1.1 What is the principal data protection legislation?

Personal data protection legislation in Indonesia is not codified under certain law, instead it stipulates in various legislations in particular the legislations regarding electronic systems which discusses and stipulates quite comprehensively on personal data protection. These regulations consist of:

a. Law No. 11 of 2008 on Electronic Information and Transaction as amended by Law No. 19 of 2016 "(**Law 11/2008**").
b. Government Regulation No. 71 of 2019 on Administration of Electronic Transaction and System ("**Regulation 71/2019**").
c. Minister of Communication and Informatics Regulation No. 5 of 2020 on Private Electronic System Providers ("**Regulation 5/2020**").
d. Minister of Communication and Informatics Regulation No. 20 of 2016 on Personal Data Protection on Electronic System ("**Regulation 20/2016**").

Aside from the above regulations, the Indonesian government is currently preparing a draft of a codified personal data protection law ("**PDPL Draft**") that specifically regulates personal data protection. Although the PDPL Draft is not final and subject to further changes, there is a possibility that the PDPL Draft will be enacted as a law in the near term.

### 1.2 Is there any other general legislation that impacts data protection?

In the implementation and enforcement of data protection, general criminal provisions under the Indonesian Penal Code (*Kitab Undang-Undang Hukum Pidana*, or "**KUH Pidana**") might be used to impose penal sanction, for instance, for the personal data falsification (Article 263 or Article 264 of KUH Pidana) or violation of personal data theft (Article 362).

Furthermore, civil remedies may also be given under tort as mandated under Regulation 20/2016 where private data owners and electronic system providers may submit a lawsuit for failure of the personal data protection. In general, tort claim in Indonesia is governed under the Indonesian Civil Code (*Kitab Undang-Undang Hukum Perdata*, or "**KUH Perdata**") where it is regulated that every action that violates the law and causes losses to another person, shall impose an obligation on the person who causes such losses due to its fault to remedy such losses (Article 1365 of KUH Perdata).

### 1.3 Is there any sector-specific legislation that impacts data protection?

Yes, there are some sector-specific legislation that impact data protection, among others, in health, banking, real properties, and the capital market under the following regulations:

a. Law No. 36 of 1999 on Telecommunications as partially amended by Law No. 11 of 2020 on Job Creation.
b. Law No. 10 of 1992 on Banking as amended by Law No. 10 of 1998.
c. Law No. 8 of 1995 on Capital Markets.
d. Law No. 14 of 2008 on Disclosure of Public Information.
e. Law No. 36 of 2009 on Health.
f. Law No. 23 of 2006 on Residence Administration as amended by Law No. 24 of 2013.

Generally, in Indonesia, personal data protection is closely related to the regulations related to electronic systems. The Legalisation above tends to focus on the personal data protection in electronic systems, while non-electronic personal data protection is governed under a more general regulation or sector-specific regulation.

### 1.4 What authority(ies) are responsible for data protection?

In general, the authorities that are responsible for data protection are the Ministry of Communication and Informatics ("**MCI**"). In its task, MCI can be supported by the Indonesian police. There are also sector-specific authorities that supervise their sector in tandem with MCI such as the Bank of Indonesia for data protection in banking sector, Ministry of Health that supervises the health sector and Financial Services Authority that supervises data protection compliance in non-banking financial service institutions.

## 2 Definitions

**2.1 Please provide the key definitions used in the relevant legislation:**

- "**Personal Data**"
  Based on Article 1 number 29 of Regulation 71/2019, Personal Data is any data on a person which is identified and/or may be identified individually or combined with other information both directly and indirectly through an electronic System and non-electronic system.
- "**Processing**"
  Definition of processing is not specifically regulated under the Indonesian laws, however, based on elucidation of Article 2 paragraph (6) of Regulation 71/2019, Personal Data processing shall consist of acquisition and collection, processing and analysing, improvement and update, display, announcement, transfer, dissemination, or disclosure, and/or deletion or destruction of Personal Data.
- "**Controller**"
  Definition of controller is not specifically regulated under the Indonesian laws, however, controlling activities in relation to the collection, process, storage, publication and deletion of personal data is stipulated under Regulation 20/2016 as the activities that might be conducted by an electronic system provider. These activities are regulated under regulations related to data protection in Indonesia. The definition of electronic system provider under Regulation 71/2019 is every person, state official, business entity or public that provides, maintains and/or operates the electronic system whether individually or jointly with the electronic system user for its own interest or another party's interest. Separately, the definition of controller is defined under the PDPL Draft as a party that determines the purpose and carries out personal data processing.
- "**Processor**"
  The definition of processor is not specifically regulated under the Indonesian laws, however, similarly to controller, processor is stipulated as one of the activities carried out by an electronic system provider. On the other hand, the PDPL Draft defines personal data processor as a party that carries out personal data protection under the name of a personal data controller.
- "**Data Subject**"
  The definition of data subject is not specifically regulated, however this might be synonymous with personal data owner which is defined under Regulation 20/2016 as an individual to whom certain personal data/information is attached.
- "**Sensitive Personal Data**"
  Indonesian laws do not specifically stipulate a definition for sensitive personal data. They only define personal data in general, whereas under Regulation 71/2019 personal data is defined as every data regarding an individual whether identified and/or identifiable severally or combined with other information through an electronic or non-electronic system, whether directly or indirectly.
- "**Data Breach**"
  Data breach is not specifically defined under Indonesian legislations on data protection. However, failure of personal data protection is one of the subjects governed under Regulation 20/2016 and Regulation 71/2019. For instance, under Article 14 paragraph (5) of Regulation 71/2019, it is stipulated that if there is a failure of personal data protection, the electronic system provider must notify the personal data owner in writing. In addition, Regulation 20/2016 also provides some stipulations regarding the mitigation of personal data protection failure such as the establishment of internal policy and training within the organisation of the electronic system provider.
- **Other key definitions**
  Indonesian laws do not provide a specific definition similar to pseudonymous data, direct personal data or indirect personal data.

## 3 Territorial Scope

**3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?**

Yes, based on Article 2 of Law No. 11/2008, these data protection laws apply to any unlawful action committed by a foreign entity which triggers any legal consequence in Indonesia. For instance, if a foreign entity fails to process the personal data of an Indonesian individual appropriately or illegally, such Indonesian individual may claim for compensation to such foreign entity if its action causes damages to said Indonesian individual in accordance with Article 26 of Law No. 11/2008.

## 4 Key Principles

**4.1 What are the key principles that apply to the processing of personal data?**

- **Transparency**
  Article 14 paragraph (30) of Regulation 71/2019 stipulates that every processing of personal data must obtain approval from the personal data owner for one or more purposes that have been conveyed to the personal data owner. Article 7 paragraph (1) of Regulation 20/2016 also stipulates that obtaining and collection of personal data by an electronic system provider must be limited to the relevant information, in accordance with its purpose, and must be carried out accurately.
- **Lawful basis for processing**
  Article 12 of Regulation 20/2016 stipulates that personal data can only be processed and analysed in accordance with the purpose that the electronic data provider has clearly stated at the time the personal data is obtained and collected. Furthermore, the process and analysis of personal data can only be obtained upon consent.
  As consent is extensively emphasised under the regulations related to personal data protection, it is always advisable that every action in relation to personal data is carried out after obtaining written consent from the personal data owner.
- **Purpose limitation**
  Indonesian laws do not specifically set forth any limitation on the purpose in relation to personal data collection. However, as the purpose must be stated when the electronic system provider requires consent from the personal data owner, the purpose elaborated on such form can be deemed as an agreement. Under Article 1320 of the KUH Perdata, one of the requirements of an agreement is that the agreement is not for unlawful matters. As such, if the purpose itself is unlawful the entire collection process of personal data (including the obtained consent thereon) can be deemed as null and void.

- **Data minimisation**
  Although there is no express provision on data minimisation, Regulation 71/2019 and Regulation 20/2016 have provided that actions related to personal data can only be done within the purpose clearly conveyed to the personal data owner. Furthermore, Article 16 of Regulation 71/2019, it is also stipulated that if personal data no longer accords with the purpose of collection, the personal data must be deleted upon request from the personal data owner.
- **Proportionality**
  Indonesian laws do not provide specifically provisions regarding proportionality, but proportionality is implemented as a principle basis as can be seen from the provision regarding the purpose of utilisation of personal data. From those provisions, it could be understood that Indonesian laws tend to adopt the principle that personal data cannot be used extensively, but within the purpose agreed by the personal data owner.
- **Retention**
  Personal data processing is destroyed and/or deleted unless it is in a retention period in accordance with the need based on laws and regulations. Under Article 15 paragraph (3) of the Regulation 20/2016, the minimum storage period of personal data is five (5) years as of the date the relevant personal data owner no longer uses the electronic system, if there are no provisions of laws and regulations that specifically regulate the said matter.
- **Protection**
  Personal data processing is conducted by protecting the personal data security from loss, misappropriation, illegal access and disclosure, as well as alteration or destruction of personal data.
- **Mitigation Principle**
  Indonesian laws emphasise the importance of mitigation for failure of personal data protection where both Regulation 71/2019 and Regulation 20/2016 set forth extensive requirements for the operation of electronic system that is aimed to, among other, mitigate the failure of personal data protection. For instance, Article 5 of Regulation 20/2016, an electronic system provider must prepare internal rules to prevent the failure of personal data protection.

## 5 Individual Rights

### 5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**
  Based on Article 26 of Regulation 20/2016, a personal data owner shall be entitled to access his/her personal data without interfering with the management system of personal data, unless otherwise regulated by laws and regulations. The personal data owner is also entitled to obtain a history of his/her personal data that has been submitted to the data collector as long as it is in accordance with the laws and regulations.
- **Right to rectification of errors**
  Based on Article 26 of Regulation 20/2016, a personal data owner shall be entitled to get access to rectify or update his/her personal data without interfering with the management system of personal data, unless otherwise regulated by laws and regulations.
- **Right to deletion/right to be forgotten**
  Based on Article 26 of Regulation 20/2016, a personal data owner may request the collector data to delete or destruct his/her personal data, unless otherwise specified by the provisions of laws and regulations. Furthermore, Article 15 of Regulation 71/2019 also expressly stipulates the right to erasure and the right to delisting (to request that the personal data is excluded from the engine search) owned by a personal data owner. Article 16 paragraph (2) of Regulation 71/2019, however, provides an exemption for this right for personal data that, based on specific regulations, are prohibited from being deleted (e.g. information related to state security or financial information).
- **Right to object to processing**
  As elaborated in question 4.1 above, processing of personal data can only be carried out only if there is a consent from a personal data owner. As such, the personal data owner may reject the request of the use of his/her data by the data collector.
- **Right to restrict processing**
  Based on Article 21 of Regulation 20/2016, a personal data owner may restrict the data collector from displaying, announcing, delivering, disseminating and/or opening access to his/her data because these actions require prior consent from the data owner.
- **Right to data portability**
  Indonesian laws do not provide specification stipulation related to data portability. Although Article 26 of Regulation 20/2016 provides the right of a personal data owner to access and to receive her/his personal data history, it is not stipulated further the form of such information or access.
- **Right to withdraw consent**
  Based on Article 16 paragraph 1(b) of Regulation 20/2016, a personal data owner can withdraw its consent.
- **Right to object to marketing**
  Based on Article 21 of Regulation 20/2016, a personal data owner may restrict the dissemination of his/her data. Further, Article 44 of the Regulation 71/2019 regulates that the marketing sender must ensure that the information which is sent is valid and is not disturbing to the personal data owner.
- **Right to complain to the relevant data protection authority(ies)**
  Based on Article 26 and Article 29 of Regulation 20/2016, the personal data owner may submit a complaint over the failure of the protection of their personal data to the MCI. The complaint will be proceeded by the MCI through its Directorate General as a dispute resolution forum between a personal data owner and the electronic system provider to settle the issue amicably.
- **Other key rights**
  Based on Article 96 and Article 97 of Regulation 71/2019, the public may submit a request of termination of access of an electronic system administrator to electronic information and/or document if they violate the provision of laws and regulations, for instance illegally accessing personal data of a certain individual.
  Furthermore, under Article 32 of Regulation 2016, a personal data owner may also submit a lawsuit to claim compensation from the failure of personal data protection if the dispute resolution within MCI cannot be solved amicably. In relation to this, generally even if a personal data owner does not submit a complaint to MCI first, the personal data owner can directly submit a lawsuit to claim compensation to the court without prejudicing her/his right before the court.

## 6 Registration Formalities and Prior Approval

### 6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

In general, there is no legal obligation on a business to register with or notify the data protection authority in respect of its processing activities.

However, if the business conducts the personal data processing using an electronic system, which has an internet-based portal, website, or an application to process personal data for operational activities which serve the public in relation to electronic transaction activities, such business is required to register as an electronic system provider ("**ESP**") to the MCI via the Online Single Submission ("**OSS**") based on Article 2 paragraph 5 (b) (6) and Article 6 of the Regulation 71/2019.

### 6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

Registration must be specifically based on Article 3 of Regulation 5/2020. This regulates that the submission of a registration application contains the correct information regarding:

a. a general description of the operation of Electronic Systems, as follows:
   i. electronic system name;
   ii. electronic systems sector;
   iii. uniform resource locator (URL) of the website;
   iv. domain name system and/or Internet Protocol (IP) server addresses;
   v. business model description;
   vi. brief description of electronic system functions and electronic system business processes;
   vii. information about the processed personal data;
   viii. information on the location of management, processing and/or storage of electronic systems and electronic data; and
   ix. a statement stating that the electronic system provider guarantees and implements the obligation to provide access to electronic system and electronic data in order to ensure the effectiveness of supervision and law enforcement in accordance with the provisions of laws and regulations.
b. statement of obligation to ensure information security in accordance with the provisions of laws and regulations;
c. statement of obligation to protect personal data in accordance with the provisions of laws and regulations; and
d. statement of obligation to perform an electronic system feasibility test in accordance with the provisions of laws and regulations.

### 6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

Based on Article 5 of the Regulation 5/2020, ESP must make a registration per legal entity and notification of changes for any changes per system or database if there are any changes in the information provided to the MCI.

### 6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

Based on Article 2 and Article 4 of the Regulation 5/2020, this registration requirement is applicable to both local and foreign entities, including its representative office or branch office. For a foreign entity, registration is required if such entity provides its service or conducts its business activity in Indonesia and/or its electronic system is used by Indonesian customers.

### 6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

Please refer to the answer to question 6.2.

### 6.6 What are the sanctions for failure to register/notify where required?

Based on Article 100 of the Regulation 71/2019, the failure to conduct registration might be imposed with an administrative sanction in the form of the following:

a. a written warning;
b. an administrative fine;
c. temporary suspension;
d. access termination; and/or
e. exclusion from the list of registered electronic system providers.

### 6.7 What is the fee per registration/notification (if applicable)?

Until to date there are no regulations requiring a fee per registration, the registration can be made without any charge.

### 6.8 How frequently must registrations/notifications be renewed (if applicable)?

Under Indonesian laws, there is no requirement for periodic renewal. However, any changes to registration information that was submitted must be notified to the MCI.

### 6.9 Is any prior approval required from the data protection regulator?

No approval is required. However, data protection regulation, in this case the MCI, will verify all required documents and information before confirming the registration of an ESP.

### 6.10 Can the registration/notification be completed online?

Yes, it is conducted online by submitting the registration application to the MCI via OSS. OSS is a licensing and reporting system in Indonesia that integrates all licensing and administrative reporting of business in Indonesia.

**6.11 Is there a publicly available list of completed registrations/notifications?**

Yes, the list of registered electronic system providers can be accessed at https://pse.kominfo.go.id/tdpse-terdaftar.

**6.12 How long does a typical registration/notification process take?**

Indonesian laws are silent on this. However, typically it would take around one to three weeks as it would be subject to the sufficiency of documents and information submitted.

## 7 Appointment of a Data Protection Officer

**7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.**

Indonesian laws do not specifically recognise a Data Protection Officer. However, Article 28 letter (i) of Regulation 20/2016 requires that there must be a contact person who can be easily contacted by the personal data owner regarding the management of his/her personal data. As a reference only, under the PDPL Draft the requirement to appoint a Data Protection Officer is introduced and applicable for all personal data controllers and processors in certain matters which include:

a. personal data processing for public service interests;
b. personal data controller's core activity has a nature, scope and/or purpose that requires coordinated and systematic supervision on personal data on a large scale; and
c. personal data controller's core activity consisting of personal data processing on a large scale for specific personal data and/or personal data that is related to criminal action.

**7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?**

Indonesian laws do not specifically stipulate the sanction for failing to appoint a Data Protection Officer. However, under the PDPL Draft, there are administrative sanctions for a failure to appoint a Data Protection Officer consisting of written warning, temporary suspension of personal data processing activity, deletion or destruction of personal data, indemnification of losses and/or an administrative fine.

**7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?**

As elaborated in question 7.1, a Data Protection Officer is not recognised in Indonesia. A contact person required by Regulation 20/2016 is not necessarily a Data Protection Officer and usually an employee of an ESP. Such contact person does not have any protection in his roles aside from protection from employment law perspective. As a reference, protection for the Data Protection Officer is also not regulated under the PDPL Draft.

**7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?**

Indonesian laws are silent on this. With regard to the contact person mention in the preceding sections, we believe that it is possible for one party to be appointed as the contact person for multiple ESPs. As a reference, the PDPL Draft also does not stipulate any specific provision on this.

**7.5 Please describe any specific qualifications for the Data Protection Officer required by law.**

Indonesian laws are silent on this. As a reference, under the PDPL Draft, the qualifications of the Data Protection Officer stipulates that they must be appointed based on professional quality, knowledge on laws and personal data protection practice and the ability to perform her/his duty.

**7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?**

The Legislations are silent on this. As a reference, the PDPL Draft stipulates the responsibilities of the Data Protection Officer, which include:

a. informing and providing advice to the personal data controller or processor to observe the provisions under the personal data protection law;
b. supervising and ensuring compliance with the personal data protection law and policy of personal data controller or processor including assignment, responsibility, improving of awareness and training for parties who are involved in personal data processing and relevant audits;
c. providing advice regarding the assessment of personal data protection impact and supervising the performance of a personal data controller and processor; and
d. coordinating and acting as the contact person for the issues related to personal data processing, including conducting consultations regarding the mitigation of risks and/or other matters.

**7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?**

Indonesian laws are silent on this. As a reference, the PDPL Draft does not specifically stipulate on this.

**7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?**

The Legislations are silent on this. As a reference, the PDPL Draft does not specifically stipulate on this.

## 8 Appointment of Processors

**8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?**

As mentioned previously in question 2.1, Indonesian laws do not specifically recognise personal data processors. This is only

introduced in the PDPL Draft, which has not been enacted yet. However, although the general concept of personal data processor has been recognised in practice (i.e. particularly in a situation where an ESP that collects personal data appoints a third party to process personal data), the appointment of personal data processors is not a new thing in Indonesia. As a general concept, if a personal data processor is not part of an internal organisation with the ESP that collects personal data, any appointment of any third parties (including those who process personal data) must be made in some sort of an agreement to protect the interest of both parties commercially and legally. As a reference, the PDPL Draft also does not specifically stipulate about these matters.

**8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?**

By keeping in mind our elaboration in question 8.1, the agreement between the parties would actually refer to general concept of agreement in Indonesia as there is no specific requirements under the regulations related to personal data protection. Generally, Article 1320 of KUH Perdata provides that the elements of validity of an agreement are as follows:

a. consent of parties;
b. legal capability to enter into an agreement;
c. objectivity; and
d. the provision governed in the agreement is not contradictory with any social norm, public order and Indonesian laws and regulations.

It is always preferable to make the agreement in writing for the sake of evidentiary if a dispute arises. With regard to the content of the agreement, it is always advisable for a business that appoints the personal data processor to require the personal data processor carrying out strict protection of personal data and indemnify the business from any claims arising from failure to protect such personal data.

## 9 Marketing

**9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).**

Electronic marketing is regulated directly or indirectly under the Regulation 71/2019 and Government Regulation No. 80 of 2019 on Trading through Electronic System ("**Regulation 80/2019**") and Minister of Trade Regulation No. 50 of 2020 on Terms of Business Licensing, Advertising, Development and Supervision of Business Actor in Trading through Electronic System ("**Regulation 50/2020**").

Based on Articles 32 and 33 of Regulation 80/2019, a business can create and/or send electronic advertisements for marketing or promotional purposes. In carrying out such activities, a business must comply with the laws and regulations on broadcasting, protection of privacy and personal data, consumer protection, and does not conflict with the principles of fair business competition.

Furthermore, Article 44 of Regulation 71/2019 regulates that a marketing sender must ensure the information sent to its target are valid and not disturbing to the personal data owner. This is to protect the recipient from receiving disturbing electronic information (spam). Common forms of spam are e-mail spam, instant message spam, Usenet newsgroup spam, Web search-engine spam, blog spam, news spam on mobile phones, and Internet forum spam.

Article 35 of Regulation 80/2019 also regulates that a business that creates, provides facilities and/or distributes electronic advertising is obliged to ensure that the substance or material of electronic advertising that is sent does not conflict with the provisions of laws and regulations and is responsible for the substance or material of electronic advertising.

Separately, based on Article 26 of Law No. 11/2008, use of any information through electronic media that involves personal data of a person must be made with the consent of the person concerned, thus the business must obtain prior opt-in consent of the recipient. As such, electronic direct marketing activities must also observe Indonesian laws related to personal data protection.

Finally, Law No. 8 of 1999 on Consumer Protection ("**Law No. 8/1999**") may apply for marketing in general, whether or not it is carried out electronically. Article 17 of Law No. 8/1999 stipulates that a marketing business actor may not produce marketing that might:

a. mislead the consumer regarding quality, quantity, material, utility and price of goods and/or fee of services as well as the accuracy of time regarding;
b. mislead the guarantee/warranty on goods and/or services;
c. contain information that is untrue, false or inaccurate on goods and/or services;
d. does not contain information regarding the risk of utilisation of goods and/or services;
e. exploits an event and/or a person without the consent of the relevant person; or
f. violates ethics and/or laws and regulations regarding advertising.

The advertisements code of ethics ("**ACE**") itself was lastly issued on 20 February 2020 by the Indonesian Advertising Council. The ACE comprehensively sets forth the ethic of advertisements in various sectors such as alcohol, drugs, food and beverages, professional services and other sectors. Although ACE is not an instrument of law in Indonesia, the violation of ACE might still be considered as violations of law due to stipulates of Law No. 8/1999 Article 17 letter (f) above.

**9.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?**

Although it is not specified under Indonesian laws, it is understood that the restrictions are applicable to all parties, including in a business-to-consumer marketing and business-to-business context.

**9.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).**

Law No. 8/1999 along with the ACE as we elaborated above in question 9.1 applies for marketing via other means.

**9.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?**

Yes, the restrictions above also apply to marketing sent from other jurisdictions. As for electronic marketing, the exterritorial nature of the restrictions is due to the extraterritoriality of Law No. 11/2008. On the other hand, in regard to Law No. 8/1999, it applies for the business that carries out activities within Indonesia, hence although a business from other jurisdictions does not have representatives in Indonesia, it could be subject to Law No. 8/1999 as it carries out activities in Indonesia (i.e. carrying out marketing in Indonesia).

**9.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?**

In practice, if it relates to electronic marketing, the MCI will generally be active if there is any complaint. However, if it relates to non-electronic marketing, any complaint might be submitted to the general authorities in Indonesia such as the police, and in addition the complaint can also be submitted to known institutions regarding consumers in Indonesia such as *Yayasan Lembaga Konsumen Indonesia* or institutions regarding advertising such as the Indonesian Advertising Council.

**9.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?**

It might be unlawful if the marketing lists themselves were obtained without proper consent from the relevant data owner in the marketing lists. It is advisable to ensure that the third parties that provide the marketing lists have obtained proper consent for transferring the marketing list (and any personal data contained therein) from the relevant parties. Proper checking of consent documentations from third parties is advisable prior to purchasing the marketing list.

**9.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?**

The maximum penalties are set forth in Law No. 8/1999 where the violation of Article 17 as we elaborated in question 9.1 could be sanctioned with imprisonment of a maximum of five years or fine of a maximum of IDR2,000,000,000.

## 10 Cookies

**10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).**

There is no legislation that specifically restricts cookies. However, if the extent of cookies would include personal data, the cookies themselves would be subject to Indonesian laws related to personal data protection.

**10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?**

As we elaborated in question 10.1 above, although the restriction does not specifically govern the cookies, Indonesian laws on personal data protection would apply if the cookies involve collection of personal data.

**10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?**

To date, we are not aware of any news on the enforcement actions taken by the authority in relation to cookies.

**10.4 What are the maximum penalties for breaches of applicable cookie restrictions?**

There are no specific laws and regulations on the restriction of the use of cookies, but the general laws and regulations on personal data protection can apply. If there is any breach of the laws on personal data protection, the maximum penalty for any personal data breach is termination of access (i.e. access blocking, account closure, and/or removal of content), excluded from the list and/or announcements on sites online based on Regulation 20/2016 and Regulation 71/2019.

## 11 Restrictions on International Data Transfers

**11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.**

Based on Article 22 Regulation of 20/2016, transfer of personal data to other jurisdictions requires the following actions:

a. coordinate with the MCI to conclude this matter; and
b. implement the provision of laws and regulations on cross-country private data exchange.

Coordination of question 11.1 (a) above is conducted by the following means:

a. submitting a report on the implementation of the transfer of private data, at least shall contain the destination country, name of recipient, date of implementation, purpose of transfer;
b. requesting for advocacy, if necessary; and
c. submitting a report on the performance of activity.

**11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).**

Typically, the consent to transfer personal data abroad would be included at the initial consent request when a business collects personal data. Hence, once the personal data is collected along

with the consent from a personal data owner, a business could transfer the personal data abroad. Usually the transfer is made to the business' affiliates overseas or a third-party data processor overseas.

However, in practice, the implementation of compliance with the requirement which we spoke of in question 11.1 is still rather low. As such, it is still a common case in Indonesia for a business to transfer personal data abroad without coordination with the MCI.

**11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.**

As we elaborated in question 11.1 above, strictly speaking, notification authority is required. However, aside from the requirements elaborated in question 11.1, Indonesian laws are still unclear on the procedure of the notification itself. There is no further provision on how the notification should be made, how the MCI would acknowledge the notification, whether the MCI needs to verify the notification and other matters regarding the procedures of notification.

**11.4 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?**

This is not applicable to the laws of Indonesia.

**11.5 What guidance (if any) has/have the data protection authority(ies) issued in relation to the European Commission's revised Standard Contractual Clauses?**

This is not applicable to the laws of Indonesia.

## 12 Whistle-blower Hotlines

**12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?**

Indonesian laws are silent on this matter. In practice, the corporate whistle-blower hotline is commonly regulated under the internal policy of the relevant company. The scope could be related to corruption, compliance of internal rules of a company and other matters related to compliance in general.

**12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?**

The Indonesian laws are silent on this matter. This would be subject to the corporate whistle-blower policy. In practice, anonymous reporting is discouraged because the management of a company would need to confirm the identity of the reporting party for the purpose of verification of the report. If the identity of the reporting party is not disclosed, it would be difficult to verify the validity of the report itself.

This practice is also implemented by the Indonesian authorities, for instance the Indonesian Commission Eradication Corruption ("**KPK**"). KPK requires the identity of the reporting party, such as name, address, telephone number, copy identity card, etc.

Although disclosure of identity is encouraged, the confidentiality of the whistle-blower itself would usually be strictly maintained by a company or authority for protection purposes. The guarantee on identity confidentiality is usually implemented to encourage whistle-blowing activities in itself.

## 13 CCTV

**13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?**

No, the use of CCTV does not require separate registration/notification or prior approval from the relevant data protection authorities.

**13.2 Are there limits on the purposes for which CCTV data may be used?**

Indonesian laws do not specifically limit the purpose of CCTV, however, as images captured by CCTV might be personal data, the use of CCTV would in itself be subject to personal data protection regulations.

Regarding the use of CCTV in the private sector, the business/CCTC owner must consider the other's privacy and require prior approval from the relevant party. Based on Article 26 of Law No. 11/2008, any use of information through electronic media which relates to an individual's personal data must require approval from the relevant party. Any individual who assumes that his/her rights are infringed due the use of electronic media, including CCTV, may submit claim to such CCTV owner.

Implementing this into practice, where the images resulting from CCTV are to be published, certain censorship might be required if the owner of such images (e.g. faces, house floor plan, vehicle number, etc.) does not provide consent for such publication.

## 14 Employee Monitoring

**14.1 What types of employee monitoring are permitted (if any), and in what circumstances?**

Indonesian laws are silent on this. However, the Indonesian labour laws impliedly recognise the necessity of an employer to know the basic information of the employee for the employer's verification. It is also generally permitted to monitor the employee during working hours within the work premises to ensure their performance, security, safety and health. Any further extent of monitoring would be preferably carried out upon consent of the relevant employee.

**14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.**

Yes, consent and notice are generally required and advisable. The employers will typically obtain the consent and provide notice from the work agreement between the employer and employee.

**14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?**

The labour union/employee representatives shall be notified or consulted in the event that if there are any issues on the rights and interests of employees based on Article 25 of Law No. 21 of 2000 on Labour Union, as follows:

a. Negotiate a collective labour agreement with the employer.
b. Represent employees in industrial dispute settlements.
c. Represent employees in manpower institutions.
d. Establish an institution or carry out activities related to efforts to improve employees' welfare.
e. Carry out other manpower- or employment-related activities that do not violate the applicable laws and regulations.

## 15 Data Security and Data Breach

**15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?**

Based on Article 25 of the Regulation 20/2016, the ESP has the obligation to ensure the security of personal data. Indonesian laws provide a list of requirements for an ESP for the purpose of, among others, ensuring the protection of personal data and minimising any risk of personal data protection failure. The list of requirements are, among others:

a. to undergo certification process for electronic systems under its management in accordance with the provisions of laws and regulations;
b. to safeguard the authenticity, validity, confidentiality, accuracy and relevance as well as the conformity with the purpose of acquiring, collecting, processing, analysing, storing, displaying, announcing, delivering, disseminating and erasing personal data;
c. to notify the subjects in the event of a failure of personal data confidentiality protection in the electronic system under its management, subject to the following provisions on the said notification;
    i. should be accompanied with the reasons or causes of the failure of personal data confidentiality protection;
    ii. may be carried out electronically if the subjects have granted an approval for it which has been declared at the time the acquisition and collection of their personal data take place;
    iii. should ascertain that it has been received by the subjects if such a failure contains potential harm against the party concerned; and
    iv. a written notice should be sent to subjects no later than 14 days after the failure is known.
d. to have internal regulations relating to the protection of personal data which conform with the provisions of laws and regulations;
e. to provide audit track records on all electronic system organisation activities that are under its management;
f. to provide options to the subjects whether the personal data it manages may or may not be used and/or displayed by/to any third party based on an approval as long as it still relates to the purpose of acquiring and collecting personal data;
g. to grant access or opportunity to the subjects to alter or renew their personal data without disrupting the personal data management system, unless stipulated otherwise by the provisions of laws and regulations;
h. to dismiss personal data in accordance with the provisions of this ministry regulation or the provisions of other laws and regulations which specifically regulates each supervisory institution and sector administrator as regards the said matter; and
i. to provide a contact who can be easily contacted by the subjects regarding the management of their personal data.

**15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

Article 24 of Regulation 71/2019 requires that if there is an electronic system failure or disturbance which may cause personal data protection failure, the ESP shall immediately report in the first place to the law enforcement (e.g. Indonesian police) and MCI. There is no further regulations regarding the detail of the report, but in practice, the report should generally at least contain the information that must be accompanied by reasons or causes for the failure to protect the confidentiality of personal data and could be added with the mitigation measures which have been carried out.

**15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

Yes, based on Article 28 paragraph c of Regulation 20/2016 and Article 14 of Regulation 71/2019, if there is any failure on the protection of personal data in the electronic system, the ESP must notify the data subjects in writing in the event of a failure of personal data confidentiality protection. Such notification shall:

a. be accompanied with the reasons or causes of the failure of personal data confidentiality protection;
b. be carried out electronically if the data subjects have granted an approval for it which has been declared at the time the acquisition and collection of their personal data take place;
c. be actually received by the personal data owner if such a failure threatens a potential harm against the personal data owner (the ESP must ensure such receipt by the personal data owner); and
d. be sent in writing to the data subjects no later than 14 days after the failure is known.

**15.4 What are the maximum penalties for data security breaches?**

Indonesian laws and regulations do not impose penalties for data security breaches to the ESP (including its data collector, processor or controller). However, Indonesian laws recognise and even state clearly that the personal data owner may submit a lawsuit in the event of failure of personal data protection.

In addition, Indonesian laws impose penalties to a party, who purposely and without authority or unlawfully conduct any of the following actions:

a. access computers and/or electronic systems of other persons in any manner whatsoever based on Article 30 paragraph (2) of Law No. 11/2008;

b. access computers and/or electronic systems of other persons in any manner whatsoever with the intent to obtain electronic information and/or electronic Records based on Article 30 paragraph (2) of Law No. 11/2008;
c. access Computers and/or Electronic Systems in any manner whatsoever by breaching, hacking into, trespassing into, or breaking through security systems Article 30 paragraph (3) of Law No. 11/2008; or
d. alters, adds, reduces, transmits, tampers with, deletes, moves, hides Electronic Information and/or Electronic Records of other Persons or of the public that result in any confidential Electronic Information and/or Electronic Record being compromised such that the data becomes accessible to the public in its entirety in an improper manner system based on Article 32 paragraph (3) of Law No. 11/2008.

For each of the actions listed above, the maximum penalties are imprisonment of a maximum of 10 (ten) years and/or a fine of a maximum Rp5,000,000,000 (five billion rupiah) based on Article 48 paragraph (3) of Law No. 11/2008.

## 16 Enforcement and Sanctions

### 16.1 Describe the enforcement powers of the data protection authority(ies).

i. **Investigative Powers**:
Based on Article 43 of Law No. 11/2008, the government (Indonesian Police and/or Civil Servant Investigator (*Pejabat Pegawai Negeri Sipil*)) is entitled to carry out an investigation with respect to the crime related to information technology and electronic transaction, including data protection. In carrying out an investigation, the government is authorised to conduct the following actions:
   a. summon any individual or other party to be examined as the suspect or witness with respect to allegation of crime action under this law;
   b. carry out an examination towards an individual and/or business entity which is duly suspected of committing a crime action under this law;
   c. carry out an examination towards tools and/or a facility related to information technology which was suspected of being used for committing a crime action under this law;
   d. ask for an expert's assistance for investigation; and/or
   e. cease the investigation over crime action under this law based on the prevailing criminal procedure law.

ii. **Corrective Powers**: Based on Article 36 of Regulation 20/2016, the government is entitled to issue a verbal warning and/or a written warning to the individual or business entity which obtains, collects, processes, analyses, stores, displays, announces, delivers and/or disseminates personal data illegally or not in accordance with this regulation or other prevailing laws and regulations.
iii. **Authorisation and Advisory Powers**: Based on Article 34 of Regulation 20/2016, advisory powers vested by the government is giving education service to the society regarding personal data, including consent of use of personal data, definition of personal data, rights and obligation of the data owner and electronic system administrator, and dispute settlement procedure if there is any failure of personal data protection.
iv. **Imposition of Administrative Fines for Infringements of Specified GDPR Provisions**: Based on Article 100 of Regulation 71/2019, if the ESP (or its data collector, processor or controller) fails to process the collected personal data appropriately based on the purpose of collection, it may be imposed with administrative fines. However, this regulation does not specify further regarding the amount of administrative fines and procedure to impose this sanction.
v. **Non-compliance with a Data Protection Authority**: Based on the Regulation 71/2019, this action may lead to the imposition of administrative sanction as specified in question 15.4 above.

### 16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The authority does not generally issue a ban on a particular processing activity. However, the authority may block or restrict the access to certain electronic systems (e.g. access blocking, account closure, and/or removal of content) based on Article 36 of Regulation 20/2016 and Article 100 paragraph (2) of Regulation 71/2019. Such temporary ban and access termination does not require a court order since this is in the form of administrative sanctions. However, the authority's decision to carry out such blocking or restriction can be appealed by the relevant party through, for instance, the administrative court.

### 16.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

In 2020, there have been a series of data leakage cases occurred in some e-commerce platforms (typically due to hackers). In these cases, the authority summoned the representative of the private companies to ask for clarification regarding the data leakage. We understand that, in light of the recent cases, the authority would still take a soft approach to any personal data protection failure case instead of immediately taking authoritative action such as imposing sanctions.

### 16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

Yes, the authority can exercise its power against businesses established in another jurisdiction and the enforcement is in the form of access termination or restriction of the electronic system in Indonesia.

## 17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

### 17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

From an Indonesian laws perspective, unless there are certain treaties between the countries, a business is not generally obliged to respond to foreign authorities. In such case, it would be subject to the discretion of each business whether to respond to the request from a foreign authority. Typically, a business that is a subsidiary of a company that is subject to certain jurisdiction will respond to the request from a foreign authority authorised within the jurisdiction of its parent company. In responding to

such request, a business would usually ensure whether the disclosure to the foreign authority has been included as the purpose of personal data collection or the scope of consent provided from the personal data owner. If it has not been included, usually separate consent must would be collected from the business.

In addition, the request of a foreign authority might also be enforceable if such request is admitted by the Indonesian laws. The admission of request by Indonesian laws is usually due to bilateral or multilateral treaties between countries. For instance, the Government of Indonesia has signed the International Tax Agreement, in which the foreign government may request for exchange of data related to individuals' or legal entities' income to Indonesia Director General of Tax under the Ministry of Finance. This exchange procedure is further regulated in the Director General of Tax Regulation No. Per-28/PJ/2017 on Procedure of Exchange of Information on Request Basis For the Purpose of Implementing International Agreement ("**Regulation 28/2017**").

### 17.2 What guidance has/have the data protection authority(ies) issued?

Indonesian laws do not specifically provide guidance on this.

## 18 Trends and Developments

### 18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

In 2020, there were a series of data leakage cases in private companies such as e-commerce platforms by hackers. The hackers stole data, which included account names, e-mail addresses, birth dates, telephone numbers, and several other personal data, and sold it to the dark forum. The private companies have reported this data leakage by hackers to the Indonesian Police and the investigation is still on-going.

Pursuant to data leakage in one of the biggest e-commerce enterprises in Indonesia, a lawsuit has been submitted against such company and MCI by an independent consumer community.

In addition, in 2020 the Indonesian government also introduced a new regulation on the registration as an ESP for a foreign entity. This regulation is seen as a strong gesture from the Indonesian government that the personal data protection in Indonesia is also applicable for foreign company. MCI has also conducted an active campaign in encouraging businesses in Indonesia who uses an electronic system as part of its business scheme to register as ESP in MCI to strengthen supervision in personal data protection.

### 18.2 What "hot topics" are currently a focus for the data protection regulator?

The Indonesian government is still carrying out a series of discussions between stakeholders regarding the PDPL Draft. It was said that the PDPL Draft would be enacted in early 2021; however, we have not seen any strong indication that the new law will be enacted until at least April 2021.

**Steffen Hadi** is the founding partner of H & A Partners (in association with Anderson Mōri & Tomotsune) ("**H&A**"). He is an experienced corporate commercial lawyer admitted in Indonesia and New York State. He graduated as valedictorian from Parahyangan Catholic University and obtained an LL.M. Degree from the University of Pennsylvania Law School and Wharton Business and Law of Wharton Business School. He is a member of the Indonesian Bar Association (PERADI).

Steffen has considerable experience in working with many foreign and local sponsors or investors especially in various high profile investment projects and corporate transactions in Indonesia. He also handles a number of high profile TMT projects which include assisting high-profile clients in establishing new telematics business models, investment in several start-ups in Indonesia and creating a scheme for compliance with personal data protection regulations for one of the world's biggest video game companies.

His publications include *A long wait for data protection law: Will it be effective – Jakarta Post* and *Demystifying uncharted cryptocurrency – Jakarta Post* among others.

**H & A Partners**
**in association with Anderson Mōri & Tomotsune**
Menara Astra, 39th Floor
Jl. Jendral Sudirman Kav. 5–6
Jakarta 10220
Indonesia

Tel: +62 21 5058 1861
Email: steffen.hadi@amt-law.com
URL: www.amt-law.com/en

**Sianti Candra** is a senior associate at H&A. Prior to joining H&A, she practised at prominent law firms in Indonesia. She obtained her Bachelor of Law and Master of Law Degrees from Pelita Harapan University (UPH), Indonesia. Practising for more than nine years, Sianti specialises in dispute resolution, competition law, employment law and technology, media, and telecommunication (TMT). She has handled several high-profile commercial litigation and employment dispute cases in various stages of proceedings from district court, high court and Supreme Court. Sianti is a skilled commercial lawyer and litigator.

**H & A Partners**
**in association with Anderson Mōri & Tomotsune**
Menara Astra, 39th Floor
Jl. Jendral Sudirman Kav. 5–6
Jakarta 10220
Indonesia

Tel: +62 21 5058 1861
Email: sianti.candra@gmail.com
URL: www.amt-law.com/en

**Dimas Andri Himawan** is an associate at H&A. Prior to joining H&A, Dimas was an associate of a prominent law firm in Indonesia. With more than five years of experience, he has handled a wide range of matters, which includes foreign direct investment, general corporate matters, real estate transaction, conducted legal due diligence for the purpose of M&A and human capital service matters. His specialisation includes labour law and corporate commercial transactions. Dimas has also been involved in several TMT projects for foreign investors and local companies such as acquisition of electronic services provider of one of the pioneers of the crowdsourcing enterprise in Indonesia.

**H & A Partners**
**in association with Anderson Mōri & Tomotsune**
Menara Astra, 39th Floor
Jl. Jendral Sudirman Kav. 5–6
Jakarta 10220
Indonesia

Tel: +62 21 5058 1861
Email: dimasandri.himawan@amt-law.com
URL: www.amt-law.com/en

H & A Partners (in association with Anderson Mōri & Tomotsune) ("**H&A**") is a corporate law firm that advises international and local clients in a wide range of transactions both domestic and cross-border.

Supported by its association with Anderson Mōri & Tomotsune, H&A is featured with a wide network of expertise distributed throughout the Asia Pacific region, that are fully capable of providing comprehensive support for clients in both domestic and global scale transactions.

Established in May 2020, with its experienced and talented lawyers, H&A has been highly praised by clients for its dedicated, prompt and commercial approach, as well as accurate yet practical solution for clients. H&A has handled a number of high-profile transactions, which include cross-border merger and acquisition, banking and finance, real estate, TMT and private equity funding.

H&A provides services in general corporate commercial, merger & acquisition, real estate, employment, banking & finance, competition & antitrust, business restructuring, telecommunications, media & technology, private equity investment, compliance audit and commercial dispute resolution.

**www.amt-law.com/en**

H & A Partners
in association with Anderson Mōri & Tomotsune

# Ireland



Colin Rooney


Aoife Coll

Arthur Cox LLP


## 1 Relevant Legislation and Competent Authorities

### 1.1 What is the principal data protection legislation?

The primary data protection legislation in Ireland is Regulation (EU) 2016/679 (the "**GDPR**"), and the Data Protection Acts 1988 to 2018 (together the "**DPA**"). Irish law-specific requirements which are required or provided for under the GDPR, are set out in the Data Protection Act 2018. The Data Protection Act 2018 also implements Directive (EU) 2016/680, the Law Enforcement Directive.

### 1.2 Is there any other general legislation that impacts data protection?

Yes. The following legislation also impacts data protection in Ireland:

- The Freedom of Information Act 2014 provides a legal right for persons to access information held by a body to which FOI legislation applies.
- The Protected Disclosures Act 2014 (the "**Protected Disclosures Act**") provides employment protections and certain legal immunities to workplace whistle-blowers.
- The Criminal Justice (Mutual Assistance) Act 2008, Part 3 enables Ireland to provide or seek various forms of mutual legal assistance to or from foreign law enforcement agencies.

Data protection in the electronics communications sector is also subject to S.I. No. 336/2011 the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (the "**ePrivacy Regulations**"). The ePrivacy Regulations apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communication networks in Ireland and where relevant, in the EU. The ePrivacy Regulations also contain provisions relating to electronic marketing.

### 1.3 Is there any sector-specific legislation that impacts data protection?

The following sector-specific legislation impacts data protection:

- S.I. No. 18/2021 – Data Protection Act 2018 (Section 36(2)) (Health Research) (Amendment) Regulations 2021.
- S.I. No. 534/2020 – Data Protection Act 2018 (section 60(6)) (Central Bank of Ireland) Regulations 2020.
- S.I. No. 730/2020 – Protection of Employees (Employers' Insolvency) Act 1984 (Transfer of Personal Data) Regulations 2020.
- S.I. No. 537/2019 – Data Protection Act 2018 (Section 60(6)) (Central Bank of Ireland) Regulations 2019.
- S.I. No. 188/2019 – Data Protection Act 2018 (Section 36(2)) (Health Research) (Amendment) Regulations 2019.
- S.I. No. 314/2018 – Data Protection Act 2018 (Section 36(2)) (Health Research) Regulations 2018.
- S.I. No. 82/1989 – Data Protection (Access Modification) (Health) Regulations 1989, which outline certain restrictions in the right of access relating to health data.
- S.I. No. 83/1989 – Data Protection (Access Modification) (Social Work) Regulations 1989, which outline specific restrictions in respect of social work data.

### 1.4 What authority(ies) are responsible for data protection?

The Data Protection Commission of Ireland (the "**DPC**"). The DPC is responsible for enforcing the GDPR and the DPA.

## 2 Definitions

### 2.1 Please provide the key definitions used in the relevant legislation:

- "**Personal Data**"
  Any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- "**Processing**"
  Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- "**Controller**"
  The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

- "**Processor**"
  A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
- "**Data Subject**"
  An identified or identifiable living natural person who is the subject of relevant personal data.
- "**Sensitive Personal Data**"
  The term "Sensitive Personal Data" was replaced under the GDPR with the term "Special Categories of Personal Data", being personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, and data concerning health or sex life and sexual orientation.
- "**Data Breach**"
  A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
- *Other key definitions – please specify (e.g., "Pseudonymous Data", "Direct Personal Data", "Indirect Personal Data")*
  "Pseudonymous Data", "Direct Personal Data" or "Indirect Personal Data" are not defined under Irish law. "Pseudonymisation" means the processing of personal data in such a manner that the personal data can no longer be attributed to a data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

## 3 Territorial Scope

### 3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The GDPR applies to organisations that are established in Ireland (or any EU Member State), that process personal data (regardless of whether the processing takes place in the EU). An organisation that is not established in any EU Member State, but is subject to the laws of an EU Member State by virtue of public international law, must also comply with the GDPR. The GDPR applies to organisations located outside the EU if they (either as controller or processor) process the personal data of EU residents through:

(i) offering of goods or services (whether or not in return for payment) to such EU residents; or
(ii) monitoring of the behaviour of such EU residents (to the extent that such behaviour takes place in the EU).

## 4 Key Principles

### 4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  Transparency demands that data processing be undertaken in a transparent manner and data subjects are provided with certain information in relation to the processing of their personal data. This information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and precise language. Data subjects must be provided with this information at the time of collection of the personal data, or if the personal data is collected from a source other than the data subject, within a reasonable time period after obtaining the personal data (and at the latest within one month).
- **Lawful basis for processing**
  Processing of personal data must be grounded on one or more lawful bases under Article 6 GDPR. The following lawful bases are the most relevant for organisations:
  (i) prior, freely given, specific, informed and unambiguous consent of the data subject. It must be as easy to withdraw consent as it was to give consent;
  (ii) contractual necessity (i.e. the processing is necessary for the performance of a contract to which the data subject is a party, or for the purposes of pre-contractual measures taken at the data subject's request);
  (iii) compliance with legal obligations (i.e. the controller has a legal obligation to perform the relevant processing); or
  (iv) legitimate interests (i.e. the processing is necessary for the purposes of legitimate interests of the controller or a third party except where those interests are overridden by the interests, fundamental rights or freedoms of the data subjects).
- **Purpose limitation**
  Purpose limitation is the principle that personal data is processed only for the particular purpose(s) for which it was collected (and for closely related purposes)). Personal data must not be further processed in a manner that is incompatible with those purposes. If a controller wishes to use the relevant personal data in a manner that is incompatible with the purposes for which they were initially collected, it must:
  (i) inform the data subject of such new processing before such processing is undertaken; and
  (ii) be able to rely on a lawful basis.
- **Data minimisation**
  Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed.
- **Proportionality**
  See "Data Minimisation" above.
- **Retention**
  Personal data is not to be kept in an identifiable form for any longer than the purposes for which it was collected (subject to certain limited exceptions).
- *Other key principles – please specify*
  - **Accountability**
    The principle of accountability requires that controllers are able to demonstrate compliance with each of their obligations under the GDPR.
  - **Integrity and confidentiality**
    This principle requires that technical and organisational security measures be put in place to ensure personal data is protected from various forms of data breaches.

## 5 Individual Rights

### 5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**
  A data subject has the right to obtain from a controller the following information in respect of the data subject's personal data:

(i) confirmation of whether the controller is processing the data subject's personal data;
(ii) information about the purposes of the processing;
(iii) information about the categories of data being processed;
(iv) information about the categories of recipients with whom the data may be shared;
(v) information about the period for which the data will be stored (or the criteria used to determine that period);
(vi) information about the existence of the rights to erasure, to rectification, to restriction of processing and to object to processing;
(vii) information about the existence of the right to make a complaint to the relevant data protection authority;
(viii) where the data were not collected from the data subject, information as to the source of the data; and
(ix) information about the existence of, and an explanation of the logic involved in, any automated decision-making that has a significant effect on the data subject.

The information must be provided to the data subject free of charge and within one month of receipt of the request (except in certain limited circumstances wherein the deadline may be extended by a further two months).

The data subject may also request a copy or a summary of the personal data being processed. The DPA contain exceptions to data subject rights, including the right of access. The restrictions on the right of access include where the personal data is legally privileged. Under Article 15(4) GDPR the right of access to personal data must not adversely affect the rights and freedoms of others.

- **Right to rectification of errors**
  Controllers must ensure that inaccurate or incomplete data is erased or rectified.
- **Right to deletion/right to be forgotten**
  Data subjects have the right to have their personal data where:
  (i) the personal data is no longer necessary for the original purpose for which it was collected (and no new lawful basis for such processing exists);
  (ii) if the lawful basis for the processing is the data subject's consent, the data subject withdraws that consent, and no other lawful basis for such processing exists;
  (iii) the data subject exercises his/her right to object to processing, and the controller has no overriding grounds for continuing the processing;
  (iv) the personal data has been unlawfully processed;
  (v) erasure is necessary for compliance with EU law or national data protection law to which the controller is subject; or
  (vi) if the data subject is a child, the personal data has been collected in relation to the offer of information society services.
- **Right to object to processing**
  Data subjects have the right to object to processing of their personal data where the lawful basis for that processing is public interest or legitimate interest. Where a data subject relies on this right, the controller must cease processing unless it can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the relevant data subject or requires the data in order to establish, exercise or defend legal rights.
- **Right to restrict processing**
  Data subjects have the right to restriction of processing of personal data (i.e. the personal data may only be used for limited purposes by the controller) where:
  (i) the accuracy of the data is contested by the data subject (for as long as it takes to verify that accuracy);
  (ii) the processing is unlawful and the data subject requests restriction (where the data subject opposes erasure);
  (iii) the controller no longer needs the data for its original purpose of processing, but the data is still required by the controller for the establishment, exercise or defence of legal rights; or
  (iv) verification of overriding grounds is pending, in the context of an erasure request.
- **Right to data portability**
  In certain circumstances, a data subject has a right to receive a copy of certain of his/her personal data in a structured, commonly used and machine-readable format, and to be able to transfer (or have transferred directly on his/her behalf) his/her personal data from one controller to another.
- **Right to withdraw consent**
  A data subject has the right to withdraw his/her consent to processing at any time. Data subjects must be informed of the right to withdraw consent before consent is provided and it must be as easy for a data subject to withdraw consent as it was for the data subject to give it. The lawfulness of processing based on consent before its withdrawal is not affected by its withdrawal.
- **Right to object to marketing**
  Data subjects have the right to object to the processing of personal data for the purpose of direct marketing at any time. This includes profiling to the extent it relates to such direct marketing.
- **Right to complain to the relevant data protection authority(ies)**
  Data subjects have the right to complain to the relevant data protection authority(ies). In Ireland the data protection authority is the DPC.
- *Other key rights – please specify*
  - **Right to basic information**
    See question 4.1 (Transparency).
  - **Restrictions on data subject rights**
    None of the data subject rights set out in the GDPR is an absolute right. Each is subject to restrictions in certain circumstances, as specified in the GDPR and/or the DPA.

## 6 Registration Formalities and Prior Approval

**6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?**

No, there is no requirement on a business to register with or to notify the DPC of its data processing activities.

**6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?**

Not applicable. Please see question 6.1 above.

**6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?**

Not applicable. Please see question 6.1 above.

**6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?**

Not applicable. Please see question 6.1 above.

**6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?**

Not applicable. Please see question 6.1 above.

**6.6 What are the sanctions for failure to register/notify where required?**

Not applicable. Please see question 6.1 above.

**6.7 What is the fee per registration/notification (if applicable)?**

Not applicable. Please see question 6.1 above.

**6.8 How frequently must registrations/notifications be renewed (if applicable)?**

Not applicable. Please see question 6.1 above.

**6.9 Is any prior approval required from the data protection regulator?**

Not applicable. Please see question 6.1 above.

**6.10 Can the registration/notification be completed online?**

Not applicable. Please see question 6.1 above.

**6.11 Is there a publicly available list of completed registrations/notifications?**

Not applicable. Please see question 6.1 above.

**6.12 How long does a typical registration/notification process take?**

Not applicable. Please see question 6.1 above.

## 7 Appointment of a Data Protection Officer

**7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.**

It is mandatory to appoint a Data Protection Officer ("**DPO**") for public authorities and for organisations whose core activities consist of: (i) data processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or (ii) data processing on a large scale of special categories of data or personal data relating to criminal convictions and offences.

There is no requirement under Irish law to appoint a DPO outside of the requirements set out in the GDPR.

**7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?**

An administrative fine of up to €10 million or 2% of worldwide annual turnover.

**7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?**

Yes. The DPO cannot be dismissed or penalised for performance of his/her tasks as the DPO is an independent advisory function.

**7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?**

Yes. A group of undertakings may appoint a single DPO. The DPO must be easily accessible from each undertaking.

**7.5 Please describe any specific qualifications for the Data Protection Officer required by law.**

The DPO should have an expert knowledge of data protection law and practices and the ability to carry out his/her required tasks. An organisation is required to support the DPO by providing resources necessary for the DPO to carry out his/her tasks. The DPC has published guidance on its website on the role of DPOs including the relevant skills and expertise a DPO should have.

**7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?**

A DPO should be involved in all issues relating to the processing of personal data. The GDPR outlines the minimum tasks that a DPO should have:

(i) informing and advising a controller, processor and their employees who process personal data, of their obligations under the GDPR;

(ii) monitoring compliance with the GDPR, national data protection legislation and internal policies regarding the processing of personal data, including awareness-raising and training of staff;

(iii) advising on data protection impact assessments; and
(iv) cooperating with the DPC and acting as a contact point for the DPC.

**7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?**

Yes. The DPO must be registered with the DPC.

**7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?**

No. Contact details must be provided but it is not necessary to name the DPO.

## 8 Appointment of Processors

**8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?**

Yes. A controller and processor are required to enter into a written agreement. This agreement must contain certain specific provisions that are set out in Article 28 GDPR as well as information in relation to the subject matter for processing, the duration of processing, the nature and purpose of processing, the types of personal data and the categories of data subjects.

**8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?**

It is necessary to enter a binding written agreement. This should set out the subject-matter, duration, nature and purpose of the processing. The agreement should also cover the type of personal data and categories of data subjects and the obligations and rights of the controller.

As set out in Article 28 GDPR, the terms of the agreement must require that the processor:

(i) only acts on the documented instructions of the controller;
(ii) ensures the security of the personal data processed;
(iii) complies with the requirements in respect of appointing sub-processors;
(iv) implements measures to assist the controller with responding to the exercise of data subjects' rights;
(v) assists the controller in complying with its data security, breach notification and data protection impact assessment obligations;
(vi) returns or destroys the personal data at the end of the processing relationship (except as required by law); and
(vii) provides the controller with all information necessary to demonstrate compliance with the GDPR, this includes allowing for and contributing to audits.

The processor must also ensure that the persons authorised to process personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

## 9 Marketing

**9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).**

The rules in relation to electronic communications are set out in the e-Privacy Regulations. The principles underpinning the GDPR must also be complied with in relation to personal data processed for marketing purposes.

When email or SMS are used to send messages for direct marketing the recipient's prior opt-in consent must have been obtained. In order to rely on consent, it must be the GDPR standard of consent. There is also a soft opt-in available where an organisation is marketing its own or similar products or services to an existing customer, subject to certain requirements being met.

**9.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?**

There is also a soft opt-in for B2B emails, i.e. sending emails to an email address that reasonably appears to the sender to be an email address used mainly by the subscriber or user in the context of their commercial or official activity provided that the email relates solely to that commercial or official activity. In these circumstances, it is not necessary to obtain a recipient's prior opt-in consent.

**9.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).**

In relation to marketing materials sent by post, recipients have the right to object at any time to the processing of their personal data for direct marketing purposes. The right to object must be brought to the attention of the recipient.

It is necessary to obtain prior consent when using automatic dialling machines to fax or send messages to an individual, or making telephone calls to an individual or non-natural person's mobile telephone for direct marketing purpose.

In respect of a body corporate, the use of automatic dialling machines, fax, email or SMS for direct marketing is permitted provided that the body corporate has not recorded its objection in the National Directory Database (the "**NDD**") or it has not opted out of receipt of direct marketing.

Telephone calls for direct marketing purposes to a subscriber or user is not permitted if the subscriber or user has recorded its objection in the NDD or has opted out of receiving direct marketing.

**9.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?**

The ePrivacy Regulations are ambiguous as to whether they apply to a direct marketer based outside Ireland who sends unsolicited direct marketing communications to recipients in Ireland but it is prudent for an organisation based outside Ireland sending marketing to recipients in Ireland to assume that they do.

**9.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?**

Yes, the DPC is active in this area. In its 2020 Annual Report, the DPC state that it concluded 149 electronic direct marketing investigations in 2020 and that it prosecuted six organisations for direct marketing infringements.

**9.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?**

It is not unlawful to purchase marketing lists. However, organisations may only contact the individuals on such lists where those individuals have specifically consented to receipt of marketing communications and to the sharing of their personal data for those purposes (subject to the soft opt-in described at question 9.1 above).

In relation to telephone calls, the NDD (see question 9.2 above) contains information in relation to subscribers who have expressed a preference not to receive marketing calls to landline phone numbers, or have indicated consent to receiving such calls to mobile phone numbers. Organisations should check purchased marketing lists against the NDD before making any marketing telephone calls.

**9.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?**

Under the e-Privacy Regulations, the penalties for sending electronic communications in breach of restrictions are:

- on summary conviction, a fine of €5,000; or
- on indictment, a fine of €250,000 where the offender is a body corporate or, in the case of a natural person, a fine of €50,000.

A court order for the destruction or forfeiture of any data connected with the breach may also be issued. Each communication that amounts to a breach constitutes an independent offence under the e-Privacy Regulations.

Where a breach of the GDPR occurs in relation to marketing communications, the organisation may be subject to an administrative fine under the GDPR.

## 10 Cookies

**10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).**

The e-Privacy Regulations apply to the use of cookies. Consent is required for cookies that are not strictly necessary for the service the user has explicitly requested or for the sole purpose of carrying out the transmission of a communication over an electronic communications network. The DPC released guidance on cookies in 2020. This makes clear that users must consent to cookies that are not strictly necessary before such cookies are deployed. The level of consent is the GDPR level of consent and pre-ticked boxes or sliders will not meet this standard. Users must also be provided with clear and comprehensive information in relation to cookies.

**10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?**

As outlined at question 10.1 above, consent is not required for cookies that are strictly necessary for the provision of a service explicitly requested by the user or for the sole purpose of carrying out the transmission of a communication over an electronic communications network. All other cookies must be consented to.

**10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?**

Yes. The DPC's cookies guidance was released in April 2020. The DPC granted a six-month "grace period" to website operators to ensure compliance with the guidance. Following this, the DPC investigated and commenced enforcement action against a number of website operators. The DPC's 2020 Annual Report notes that this process of cookie investigations followed by enforcement action will continue throughout 2021.

**10.4 What are the maximum penalties for breaches of applicable cookie restrictions?**

The penalties for breaches of applicable cookie restrictions under the e-Privacy Regulations are as follows:

- on summary conviction, a fine of €5,000; or
- on indictment, a fine of €250,000 where the offender is a body corporate or, in the case of a natural person, a fine of €50,000.

A court order for the destruction or forfeiture of any data connected with the breach may also be issued. Each communication that amounts to a breach constitutes an independent offence under the e-Privacy Regulations.

As stated at question 9.7 above, there is a degree of overlap between the e-Privacy Regulations and the GDPR. Where a breach of the GDPR occurs in relation to cookies, an organisation may be subject to an administrative fine under the GDPR.

## 11 Restrictions on International Data Transfers

**11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.**

Personal data cannot be transferred from Ireland outside of the European Economic Area (the "EEA") unless one of the following applies:

(a) the personal data is transferred to a jurisdiction which the European Commission considers offers an adequate level of data protection;

(b) the transfer is made on the basis of the European Commission's Standard Contractual Clauses, which ensure an appropriate level of protection for the personal data. The European Commission released new Standard Contractual Clauses on 4 June 2021;

(c) the transfer is made on the basis of intra-group binding corporate rules ("**BCRs**"), which have been approved by the DPC or another data protection supervisory authority in another EEA jurisdiction;

(d) the transfer is made on the basis of an approved code of conduct pursuant to Article 40 of the GDPR, together with binding and enforceable commitments of the organisation in the third country to apply the appropriate safeguards, including as regards data subject rights;
(e) the transfer is made on the basis of an approved certification mechanism pursuant to Article 42 of the GDPR, together with binding and enforceable commitments of the organisation in the third country to apply the appropriate safeguards, including as regards data subject rights;
(f) the transfer is made pursuant to a legally binding and enforceable instrument between public authorities or bodies; or
(g) one of the derogations specified in the GDPR applies to the relevant transfer (in limited circumstances).

**11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).**

See question 11.1 above.

**11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.**

There is no requirement to notify the DPC of transfers of personal data to other jurisdictions made pursuant to Standard Contractual Clauses.

The DPC or another supervisory authority must approve BCRs which are intended to be used to transfer personal data outside the EEA within a corporate group. The DPC's 2020 Annual Report states that during 2020 the DPC continued to act or commenced acting as the lead reviewer in relation to 42 BCR applications.

**11.4 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?**

The DPC has not released guidance following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18).

**11.5 What guidance (if any) has/have the data protection authority(ies) issued in relation to the European Commission's revised Standard Contractual Clauses?**

The DPC has not released guidance in relation to the European Commission's draft revised Standard Contractual Clauses or in relation to the finalised Standard Contractual Clauses that were released on 4 June 2021.

## 12 Whistle-blower Hotlines

**12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?**

Public and private sector employers must ensure that existing internal whistle-blower policies, and how they address whistle-blowing, meet the requirements of the Protected Disclosures Act. The concept of 'worker' under the Protected Disclosures Act includes employees, independent contractors, trainees, agency staff, and certain individuals on work experience. The Protected Disclosures Act provides an exhaustive list of relevant wrongdoings as follows:

(a) that an offence has been, is being or is likely to be committed;
(b) that a person has failed, is failing or is likely to fail to comply with any legal obligation, other than one arising under the worker's contract of employment or other contract whereby the worker undertakes to do or perform personally any work or services;
(c) that a miscarriage of justice has occurred, is occurring or is likely to occur;
(d) that the health or safety of any individual has been, is being or is likely to be endangered;
(e) that the environment has been, is being or is likely to be damaged;
(f) that an unlawful or otherwise improper use of funds or resources of a public body, or of other public money, has occurred, is occurring or is likely to occur;
(g) that an act or omission by or on behalf of a public body is oppressive, discriminatory or grossly negligent or constitutes gross mismanagement; or
(h) that information tending to show any matter falling within any of the preceding paragraphs has been, is being or is likely to be concealed or destroyed.

**12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?**

The recipient of a protected disclosure must not disclose any information that identifies who made the protected disclosure unless:

(a) the recipient can show that he/she took all reasonable steps to avoid disclosing any such information;
(b) the recipient reasonably believes that the person making the disclosure does not object to the disclosure of any such information;
(c) the recipient reasonably believes that disclosing such information is necessary for the effective investigation of the relevant wrongdoing; the prevention of serious risk to the security of the State, public health, public safety or the environment; or the prevention of crime or prosecution of a criminal offence; or
(d) the disclosure is otherwise necessary in the public interest or is required by law.

## 13 CCTV

**13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?**

Registration or prior approval of the use of CCTV is not required from the DPC. In respect of the use of CCTV, the GDPR must be complied with. The DPC has also released specific CCTV guidance.

**13.2 Are there limits on the purposes for which CCTV data may be used?**

As set out at question 13.1 above, the use of CCTV must comply with the GDPR. The DPC's CCTV guidance sets out information in respect of transparency of such processing, the lawful basis for such processing and on data protection impact assessments.

## 14 Employee Monitoring

**14.1 What types of employee monitoring are permitted (if any), and in what circumstances?**

In Ireland, there are no specific restrictions around employee monitoring. However, as monitoring involves the processing of personal data, the principles outlined at question 4.1 above must be complied with (the principles of transparency and proportionality are of particular importance).

Employees have a legitimate expectation of privacy and any monitoring and the purposes of such monitoring should be clearly set out in a policy that is made available to employees.

The DPC's guidance on CCTV states that where possible cameras should be focused on areas of particular risk, such as cash points. CCTV recording should be limited in areas where employees have an increased expectation of privacy such as changing rooms.

**14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.**

Consent is not required. However, in order to comply with transparency obligations, employees must be notified of the existence of monitoring and the purposes for which this data is processed, including if such data will be used in the context of disciplinary proceedings (this information is usually provided through an appropriate notice). The employer must have a lawful basis for the use of CCTV monitoring.

**14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?**

The extent to which works councils/trade unions/employee representatives need to be notified of such monitoring will depend on:

(i) any agreement with the relevant body;
(ii) the likelihood that the employer will seek to rely on the CCTV data; and
(iii) whether this has been covered in the relevant employee's employment contract.

## 15 Data Security and Data Breach

**15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?**

Yes, the GDPR contains a general requirement to ensure the security of processing of personal data. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, organisations must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

Such measures may include:

(i) the ability to ensure the ongoing confidentiality, integrity and resilience of processing systems and services;
(ii) the ability to restore the availability and access to personal data in a timely manner following a technical or physical incident;
(iii) pseudonymisation and encryption of personal data; and
(iv) a process for regularly testing, assessing and evaluating the technical and organisational measures for ensuring the security of processing.

**15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

Yes, a controller must report a personal data breach without undue delay (and in any case within 72 hours of first becoming aware of the breach) to the DPC, unless the breach is unlikely to result in a risk to the rights and freedoms of the data subject(s). A processor must notify any data breach to the controller without undue delay.

The notification by the controller to the DPC is made by way of a web form and must outline the nature of the personal data breach including the categories and number of data subjects concerned. The notification must also describe the likely consequences of the personal data breach, the level of risk to data subjects and outline the measures the controller proposes to adopt to address and/or mitigate the breach.

**15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

Under the GDPR, where a personal data breach is likely to result in a high risk to the rights and freedoms of the data subjects, controllers must communicate it to affected data subjects without undue delay. This must describe in clear and plain language the nature of the personal data breach, include the name and contact details of the DPO (or point of contact), describe the likely consequences of the breach and outline the measures proposed to be taken or the measures that were taken by the controller to address and/or mitigate the breach.

The controller may not be required to notify the data subject(s) if the risk of harm is remote, the controller has taken measures to minimise the risk of harm or the notification requires a disproportionate effort.

### 15.4 What are the maximum penalties for data security breaches?

The maximum penalty is the higher of €10 million or 2% of global annual turnover. In 2020, the DPC noted that infringements of Article 32 GDPR (security of personal data) are usually capped at a lower threshold under Article 83(4) GDPR, which could suggest that they may be less serious. However, in a number of decisions released in 2020, the DPC assessed breaches of Article 32 in light of a number of factors such as the sensitivity of the data processed and the number of personal data breaches that occurred as a result of such failure.

## 16 Enforcement and Sanctions

### 16.1 Describe the enforcement powers of the data protection authority(ies).

(a) **Investigative Powers**:
Civil/Administrative sanction – The DPC (and its authorised officers) has broad powers under the DPA to enter premises, including the right to:
(i) search and inspect a premises where processing of personal data takes place and to inspect the documents, records, statements or other information found there;
(ii) require the controller or processor or employee or agent of them to produce any documents, records, statements or other information relating to the processing of personal data, and in the case of data in a non-legible form, reproduce it in a legible form;
(iii) secure for later inspection any documents, records, data equipment including any computer, in which records may be held;
(iv) inspect, take extracts, make copies or remove and retain such documents and records as considered necessary;
(v) if a person referred to in (ii) that is required to provide a particular record is unable to provide it, require the person to state to the best of that person's knowledge where the record is located or from whom it may be obtained; and
(vi) require any person referred to in (ii) above to give the authorised officer any information relating to the processing of personal data that the officer may reasonably require for performing his/her functions.
The DPC may also undertake investigations, issue enforcement notices (which may require the controller/processor to take specific steps), require the controller/processor to provide a report on any matter and, where the DPC considers that there is an urgent need to act in order to protect the rights and freedoms of data subjects, apply to the Hight Court for an order suspending, restricting or prohibiting processing.
Criminal sanction – Where a controller or processor (or any person) fails to comply with an information or enforcement notice, or obstructs or impedes, or refuses to comply with a request from an authorised officer, it shall be guilty of an offence and liable:
(a) on summary conviction, to a fine of up to €5,000 and/or imprisonment for up to 12 months; and
(b) on indictment, to a fine of up to €250,000 and/or imprisonment for up to five years.

(b) **Corrective Powers**: The DPC has a broad range of powers, including to issue warnings or reprimands for non-compliance, to order the controller to disclose a personal data breach to the data subject, to impose a permanent or temporary ban on processing and to impose an administrative fine (as below).

(c) **Authorisation and Advisory Powers**: The DPC can advise the controller, accredit certification bodies and can authorise contractual clauses, administrative arrangements and binding corporate rules, as outlined in the GDPR.

(d) **Imposition of administrative fines for infringements of specified GDPR provisions**: The GDPR provides for administrative fines which can be up to €20 million or up to 4% of an organisation's worldwide annual turnover of the preceding financial year, whichever is higher.

(e) **Non-compliance with a data protection authority**: The GDPR provides for administrative fines which can be up to €20 million or up to 4% of an organisation's worldwide annual turnover of the preceding financial year, whichever is higher. See "Criminal sanction" in relation to "Investigative Power" above.

### 16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The DPC can issue an order on a particular processing activity, including a ban on processing. Such a ban does not require a court order.

### 16.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

The DPC regularly enforces its powers. In its 2020 Annual Report, the DPC stated that on 31 December 2021 it had 83 statutory inquiries on hand, including 27 cross-border inquiries. These inquiries are a mixture of own-volition inquiries as well as being complaint-based. In 2020, the DPC released a number of decisions. In December 2020, the DPC issued its first fine in a cross-border case.

### 16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

Under the GDPR, the DPC can enforce against organisations established in other jurisdictions where such organisations come within the scope of the GDPR. The DPC can enforce its powers through an organisation's GDPR representative.

## 17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

### 17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Requests from international authorities are typically made pursuant to mutual legal assistance treaties. The Criminal

Justice (Mutual Assistance) Act 2008 sets out how Ireland engages with other countries in respect of law enforcement requests on foot of various treaties and conventions, with the aim of streamlining requests between different authorities and ensuring that adequate safeguards are in place to protect individuals. The Minister for Justice and Equality acts as the "Central Authority" for mutual assistance, confirming the validity of requests for assistance and checking that the provisions of the Criminal Justice (Mutual Assistance) Act 2008 are satisfied.

Organisations may receive direct requests from authorities outside of the mutual legal assistance process. There is more risk associated with handling such requests, such that organisations will often prefer to refer the requester to the mutual legal assistance process where they have no legal obligation to produce the records that have been requested.

### 17.2 What guidance has/have the data protection authority(ies) issued?

To date, the DPC has issued limited guidance in this area. This set out information in relation to the Law Enforcement Directive and guidance in relation to how an organisation should determine whether a matter is within the scope of the directive.

## 18 Trends and Developments

### 18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

The DPC released a number of decisions in 2020. The majority of these stemmed from investigations that were initiated in response to personal data breaches. The DPC issued its first fine in a cross-border case, fining Twitter International Company €450,000. The DPC's decisions contained a variety of enforcement measures including fines, orders to bring data processing into compliance and reprimands. In December 2020, the DPC had 83 statutory inquiries ongoing and it is expected that the DPC will issue a number of decisions in 2021.

### 18.2 What "hot topics" are currently a focus for the data protection regulator?

The processing of children's data. The DPC issued its draft Fundamentals for a Child-Oriented Approach to Data Processing (the "**Fundamentals**") in December 2020 which were open for consultation until 31 March 2021. It is expected that the DPC will issue its final version of the Fundamentals in 2021. The DPC is also expected to work with the industry to produce sectoral codes in relation to the processing of children's data.

Cookies were a special project of the DPC in 2020. In early 2020, the DPC conducted a "regulatory sweep" of some of the frequently visited websites in Ireland to establish levels of compliance with the e-Privacy Regulations. Following the completion of the sweep, the DPC produced specific and detailed cookies guidance. The DPC also investigated and commenced enforcement action against a number of website operators. The DPC has noted that the process of cookies investigations followed by enforcement action will continue throughout 2021.

**Colin Rooney** is partner in the Technology and Innovation Group of Arthur Cox in Dublin. His practice focuses on technology matters, with a particular focus on data privacy and data security and covers a broad range of work, ranging from regulatory dealings and negotiations, to compliance and counselling. His practice also has a strong emphasis on commercial IT agreements.

**Arthur Cox LLP**
Ten Earlsfort Terrace
Dublin 2
Ireland

Tel: +353 1 920 1194
Email: colin.rooney@arthurcox.com
URL: www.arthurcox.com

**Aoife Coll** is an associate on the Technology & Innovation team at Arthur Cox. Aoife regularly advises a broad range of clients including private sector, public sector and non-profit bodies on a variety of matters. Aoife advises on compliance with data protection laws, including GDPR compliance as well as on technology matters more generally.

**Arthur Cox LLP**
Ten Earlsfort Terrace
Dublin 2
Ireland

Tel: +353 1 920 1726
Email: aoife.coll@arthurcox.com
URL: www.arthurcox.com

# Isle of Man


Kathryn Sharman


Sinead O'Connor

DQ Advocates Limited

## 1 Relevant Legislation and Competent Authorities

### 1.1 What is the principal data protection legislation?

The principal data protection legislation is the Data Protection Act 2018, which is supplemented by the GDPR and LED Implementing Regulations 2018 (the "**Regulations**") as well as the Data Protection (Application of GDPR) Order 2018 and the Data Protection (Application of LED) Order 2018 (the "**Orders**").

### 1.2 Is there any other general legislation that impacts data protection?

The Regulations anticipate that the Information Commissioner (the "**ICO**") will issue a data sharing Code, a direct marketing Code and any other Codes required to be issued by the Council of Ministers. These have generally not been issued at the time of writing, although a number of the Codes of Practice previously issued by the ICO remain of relevance. The ICO has also issued a number of "Closer Look" guides to support compliance with the Regulations and the Orders.

### 1.3 Is there any sector-specific legislation that impacts data protection?

The 2016 Code of Practice on Access to Government Information imposes additional data compliance obligations on government departments and public sector workers.

### 1.4 What authority(ies) are responsible for data protection?

The ICO is the independent supervisory body for data protection. The ICO is also the supervisory body for the current Unsolicited Communications Regulations (the "**UCR**") from 2005. In addition, the ICO holds certain responsibilities in respect of the Isle of Man Government's Code of Practice on Access to Government Information and also holds an adjudication role in respect of the Freedom of Information Act 2015.

## 2 Definitions

### 2.1 Please provide the key definitions used in the relevant legislation:

- "**Personal Data**"
  The Regulations currently define personal data as meaning "any information relating to an identified or identifiable living individual". "Identifiable living individual" is further defined to mean "a living individual who can be identified, directly or indirectly, in particular by reference to: (a) an identifier such as a name, an identification number, location data or an online identifier; or (b) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual".
- "**Processing**"
  "Processing" means any operation or set of operations that is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- "**Controller**"
  "Controller" means the natural or legal person, public authority, agency or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data. This definition is, however, qualified by the Regulations so that where data is processed only: (a) for purposes for which it is required by an enactment to be processed; and (b) by means which an enactment required to be used for such processing, the controller is the person on whom the obligation to process the data is imposed by the enactment or any one of the enactments (if there are more than one). The definition is also subject to the provisions on the application of the Regulations to the Crown and to Tynwald (the Isle of Man Parliament).
- "**Processor**"
  "Processor" means a natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller.
- "**Data Subject**"
  "Data Subject" means the identified or identifiable living individual to whom personal data relates.

- "**Sensitive Personal Data**"
  "Sensitive Personal Data" are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health or sex life and sexual orientation, genetic data or biometric data. This is now referred to as "Special Category Data" for the purposes of the Regulations and the Orders.
- "**Data Breach**"
  "Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
- *Other key definitions – please specify (e.g., "Pseudonymous Data", "Direct Personal Data", "Indirect Personal Data")*
  - "**Biometric Data**" means personal data resulting from specific technical processing, relating to the physical, physiological or behavioural characteristics of an individual, that allow or confirm the unique identification of that individual, such as facial images or dactyloscopic data.
  - "**Data Concerning Health**" means personal data relating to the physical or mental health of an individual, including the provision of healthcare services, that reveal information about his or her health status.
  - "**Genetic Data**" means personal data relating to the inherited or acquired genetic characteristics of an individual that give unique information about the physiology or the health of that individual and which result, in particular, from an analysis of a biological sample from the individual in question.

## 3 Territorial Scope

### 3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The Regulations apply to the following:

- A data controller established in the Island where the personal data is processed in the context of the activities of that establishment.
- A data processor processing personal data where the data processor is established in the Island and the personal data is processed in the context of the activities of that establishment.
- A data controller or data processor processing personal data where the data controller or data processor is not established in the Island but uses equipment in the Island for processing the personal data other than for the purposes of transit through the Island.
- A data controller established outside the Island where the personal data being processed relate to an individual who is in the Island when the processing takes place and the purpose of the processing is to offer goods or services to individuals in the Island, whether or not for payment or to monitor individuals' behaviour in the Island.
- A data processor processing personal data for a data controller outside the Island or a data processor outside the Island where the personal data being processed relate to an individual who is in the Island when the processing takes place and the purpose of the processing is to offer goods or services to individuals in the Island, whether or not for payment or to monitor individuals' behaviour in the Island.

## 4 Key Principles

### 4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  Personal data must be processed lawfully, fairly and in a transparent manner. Controllers must provide certain minimum information to data subjects regarding the collection and further processing of their personal data. Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
- **Lawful basis for processing**
  Processing of personal data is lawful only if, and to the extent that, it is permitted under Isle of Man data protection law. The law provides an exhaustive list of legal bases on which personal data may be processed, of which the following are the most relevant for businesses: (i) prior, freely given, specific, informed and unambiguous consent of the data subject; (ii) contractual necessity (i.e., the processing is necessary for the performance of a contract to which the data subject is a party, or for the purposes of pre-contractual measures taken at the data subject's request); (iii) compliance with legal obligations (i.e., the controller has a legal obligation to perform the relevant processing); or (iv) legitimate interests (i.e., the processing is necessary for the purposes of legitimate interests pursued by the controller, except where the controller's interests are overridden by the interests, fundamental rights or freedoms of the affected data subjects).
- **Purpose limitation**
  Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes. If a controller wishes to use the relevant personal data in a manner that is incompatible with the purposes for which they were initially collected, it must: (i) inform the data subject of such new processing; and (ii) be able to rely on a lawful basis as set out above.
- **Data minimisation**
  Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed. A business should only process the personal data that it actually needs to process in order to achieve its processing purposes.
- **Proportionality**
  Personal data must be accurate and, where necessary, kept up to date. A business must take every reasonable step to ensure that personal data that are inaccurate are either erased or rectified without delay.
- **Retention**
  Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- **Data security**
  Personal data must be processed in a manner that ensures appropriate security of those data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- **Accountability**
  The controller is responsible for, and must be able to demonstrate, compliance with the data protection principles set out above. This includes compliance with the rights of data subjects.

## 5 Individual Rights

**5.1 What are the key rights that individuals have in relation to the processing of their personal data?**

- **Right of access to data/copies of data**
  A data subject has the right to obtain from a controller the following information in respect of the data subject's personal data: (i) confirmation of whether, and where, the controller is processing the data subject's personal data; (ii) information about the purposes of the processing; (iii) information about the categories of data being processed; (iv) information about the categories of recipients with whom the data may be shared; (v) information about the period for which the data will be stored (or the criteria used to determine that period); (vi) information about the existence of the rights to erasure, to rectification, to restriction of processing and to object to processing; (vii) information about the existence of the right to complain to the relevant data protection authority; (viii) where the data were not collected from the data subject, information as to the source of the data; and (ix) information about the existence of, and an explanation of the logic involved in, any automated processing that has a significant effect on the data subject.
  Additionally, the data subject may request a copy of the personal data being processed.
- **Right to rectification of errors**
  Controllers must ensure that inaccurate or incomplete data are erased or rectified. Data subjects have the right to rectification of inaccurate personal data.
- **Right to deletion/right to be forgotten**
  Data subjects have the right to erasure of their personal data (the "right to be forgotten") if: (i) the data are no longer needed for their original purpose (and no new lawful purpose exists); (ii) the lawful basis for the processing is the data subject's consent, the data subject withdraws that consent, and no other lawful ground exists; (iii) the data subject exercises the right to object, and the controller has no overriding grounds for continuing the processing; (iv) the data have been processed unlawfully; or (v) erasure is necessary for compliance with data protection law.
- **Right to object to processing**
  Data subjects have the right to object, on grounds relating to their particular situation, to the processing of personal data where the basis for that processing is either public interest or legitimate interest of the controller. The controller must cease such processing unless it demonstrates compelling legitimate grounds for the processing that override the interests, rights and freedoms of the relevant data subject or requires the data in order to establish, exercise or defend legal rights.
- **Right to restrict processing**
  Data subjects have the right to restrict the processing of personal data, which means that the data may only be held by the controller, and may only be used for limited purposes if: (i) the accuracy of the data is contested (and only for as long as it takes to verify that accuracy); (ii) the processing is unlawful and the data subject requests restriction (as opposed to exercising the right to erasure); (iii) the controller no longer needs the data for their original purpose, but the data are still required by the controller to establish, exercise or defend legal rights; or (iv) verification of overriding grounds is pending, in the context of an erasure request.
- **Right to data portability**
  Data subjects have a right to receive a copy of their personal data in a commonly used machine-readable format, and to transfer their personal data from one controller to another or have the data transmitted directly between controllers.
- **Right to withdraw consent**
  A data subject has the right to withdraw their consent at any time. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject must be informed of the right to withdraw consent. It must be as easy to withdraw consent as to give it.
- **Right to object to marketing**
  Data subjects have the right to object to the processing of personal data for the purpose of direct marketing, including profiling.
- **Right to complain to the relevant data protection authority(ies)**
  Data subjects have the right to lodge complaints concerning the processing of their personal data with the ICO, if the data subjects live in the Isle of Man or the alleged infringement occurred in the Isle of Man.
- **Other key rights – please specify**
  Data subjects have the right to be provided with information on the identity of the controller, the reasons for processing their personal data and other relevant information necessary to ensure the fair and transparent processing of personal data.

## 6 Registration Formalities and Prior Approval

**6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?**

Personal data must not be processed unless an entry in respect of the data controller is included in the register maintained by the ICO, subject to certain exemptions. The registration requirement also extends to data processors.

**6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?**

Registration is limited to some basic information in relation to the controller or processor, including the nature of its business and the details of the Data Protection Officer or other appropriate contact.

**6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?**

Registration is required on a "per data controller" or a "per data processor" basis.

**6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?**

The Regulations require every controller and processor to which the Data Protection (Application of GDPR) Order 2018 (the "applied GDPR") applies, to register subject to

certain exemptions which are set out in Schedule Seven to the Regulations. Section 3 above sets out the scope of the Regulations in terms of the entities to which they apply.

**6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?**

Registration is limited to some basic information in relation to the controller or processor, including the nature of its business and the details of the Data Protection Officer or other appropriate contact.

**6.6 What are the sanctions for failure to register/notify where required?**

Controllers and processors commit an offence if they process data without a registration when there is no applicable exemption, and when they fail to notify the ICO of changes to their registration information. These offences carry fines of up to £10,000 and directors may also be personally liable for offences.

**6.7 What is the fee per registration/notification (if applicable)?**

Fees are prescribed by the Treasury in the Data Protection (Fees) Regulations 2018. The fees are currently set at £70 although the ICO notes that the Council of Ministers may decide to amend that in the future. Exemptions from fees are available for relevant bodies where processing is limited to certain activities.

**6.8 How frequently must registrations/notifications be renewed (if applicable)?**

Registration must be renewed annually.

**6.9 Is any prior approval required from the data protection regulator?**

Prior approval in advance of registration is not required.

**6.10 Can the registration/notification be completed online?**

The registration can be completed online via the ICO's website.

**6.11 Is there a publicly available list of completed registrations/notifications?**

There is a publicly available list of completed registrations, which is available on the ICO's website.

**6.12 How long does a typical registration/notification process take?**

As registration can be completed online, it is an almost instant process, with the ICO then issuing an acknowledgment and payment details shortly thereafter.

## 7 Appointment of a Data Protection Officer

**7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.**

The appointment of a Data Protection Officer for controllers or processors is only mandatory in some circumstances, including where there is: (i) large-scale regular and systematic monitoring of individuals; or (ii) large-scale processing of special-category personal data. Where a business designates a Data Protection Officer voluntarily, the requirements of the GDPR apply as though the appointment were mandatory.

**7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?**

In the circumstances where appointment of a Data Protection Officer is mandatory, failure to comply may result in a penalty.

**7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?**

The appointed Data Protection Officer should not be dismissed or penalised for performing their tasks and should report directly to the highest management level of the controller or processor.

**7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?**

A single Data Protection Officer is permitted by a group of undertakings, provided that the Data Protection Officer is easily accessible from each establishment.

**7.5 Please describe any specific qualifications for the Data Protection Officer required by law.**

The Data Protection Officer should be appointed on the basis of professional qualities and should have an expert knowledge of data protection law and practices. While this is not strictly defined, it is clear that the level of expertise required will depend on the circumstances. For example, the involvement of large volumes of sensitive personal data will require a higher level of knowledge.

**7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?**

A Data Protection Officer should be involved in all issues that relate to the protection of personal data. The applied GDPR outlines the minimum tasks required by the Data Protection Officer as including: (i) informing the controller, processor and their relevant employees who process data of their obligations under the law; (ii) monitoring compliance with data protection legislation and internal policies in relation to the processing of personal data including internal audits; (iii) advising on data protection impact assessments and the training of staff; and (iv) co-operating with the data protection authority and acting as the authority's primary contact point for issues related to data processing.

**7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?**

Yes, the controller or processor must notify the data protection authority of the contact details of the designated Data Protection Officer.

**7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?**

The Data Protection Officer does not necessarily need to be named in the public-facing privacy notice. However, the contact details of the Data Protection Officer must be notified to the data subject when personal data relating to that data subject are collected.

## 8 Appointment of Processors

**8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?**

Yes. The business that appoints a processor to process personal data on its behalf is required to enter into an agreement with the processor that sets out the subject matter for processing, the duration of processing, the nature and purpose of processing and the obligations and rights of the controller (i.e., the business).

It is essential that the processor appointed by the business complies with data protection requirements.

**8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?**

The processor must be appointed under a binding agreement in writing. The contractual terms must stipulate that the processor: (i) only acts on the documented instructions of the controller; (ii) imposes confidentiality obligations on all employees; (iii) ensures the security of personal data that it processes; (iv) abides by the rules regarding the appointment of sub-processors; (v) implements measures to assist the controller with guaranteeing the rights of data subjects; (vi) assists the controller in obtaining approval from the Data Protection Officer; (vii) either returns or destroys the personal data at the end of the relationship; and (viii) provides the controller with all the information necessary to demonstrate compliance with the data protection requirements.

## 9 Marketing

**9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).**

The following provisions apply:

- Direct marketing activities must generally comply with the Regulations, and the applied GDPR and direct marketing communicated by electronic messages (including email, SMS and picture messaging) must comply with the UCR.
- Persons marketing by way of electronic mail (email, SMS or picture messaging) must obtain consent of the individual prior to transmission, or instigation of transmission, unless the conditions of a "soft opt-in" are met. The conditions of the soft opt-in are that: (i) the person marketing has obtained the relevant individual's details in the course of selling or negotiating a sale of products or services offered by such person; (ii) the direct marketing only markets the same person's similar products and services; (iii) the individual was given the opportunity to opt out of marketing when their details were first collected but did not opt out at that point; and (iv) the individual is given the opportunity to opt out on each subsequent marketing communication.
- All consent requirements under the UCR can currently be validly obtained by either opt-in or opt-out consent.

The Regulations provide that the ICO will issue a direct marketing Code to contain practical guidance in relation to the carrying out of direct marketing in accordance with the requirements of the data protection legislation. This Code has not yet been made available.

**9.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?**

The restrictions that must be adhered to are applicable in both the business-to-consumer and business-to-business contexts, provided that the marketing is targeted at an individual. There are no separate regulations.

**9.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).**

The following provisions apply:

- Direct marketing activities must generally comply with the Regulations and the applied GDPR, and direct marketing communicated by telephone calls or faxes must comply with the UCR.
- Direct marketing by post is not subject to specific regulation, but any processing of personal data for the purpose of direct marketing must be done in compliance with the principles of the Regulations and the applied GDPR.
- Persons marketing by way of live telephone calls may not make unsolicited calls if either: (i) the individual or corporation contacted has previously notified the person marketing that such calls should not be made to such individual's or corporation's telephone number; or (ii) the telephone number is listed on the register provided by the UK Telephone Preference Service (to whom the responsibility of maintaining the Isle of Man register has been delegated).
- Automated telephone marketing calls may only be made with the consent of the individual or corporation to whom such calls are directed.

The Regulations provide that the ICO will issue a direct marketing Code to contain practical guidance in relation to the carrying out of direct marketing in accordance with the requirements of the data protection legislation. This Code has not yet been made available.

**9.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?**

The ICO has a range of powers under the Regulations and the applied GDPR where breaches of marketing restrictions were due to data protection issues.

**9.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?**

The ICO has a range of powers under the Regulations and the applied GDPR where breaches of marketing restrictions were due to data protection issues.

**9.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?**

There is no legal restriction to prevent the purchase of marketing lists from third parties. A data controller would, however, have to give serious consideration to the origin of the list and the data subject's awareness that their data has been sold in this way in order to ensure compliance with the data protection requirements.

**9.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?**

There are no specific penalties set out in the current law. A person suffering damage by reason of contravention of the law is entitled to bring proceedings for financial compensation against the person contravening the law.

## 10 Cookies

**10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).**

The UCR implemented Article 13 of the European Privacy and Electronic Communications Directive (2002/58/EC) (the "**Privacy Directive**"). The UCR have not yet been amended to incorporate the changes made to the Privacy Directive regarding cookies in May 2011. As a result, the requirements of the Privacy Directive are regarded as "best practice" only on the Isle of Man, and implementation of the guidance relating to cookies remains voluntary.

**10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?**

As above, there is no specific legislation or binding guidance regarding cookies on the Isle of Man.

**10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?**

There is no evidence that the ICO has taken any enforcement action in relation to cookies.

**10.4 What are the maximum penalties for breaches of applicable cookie restrictions?**

There are no relevant penalties.

## 11 Restrictions on International Data Transfers

**11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.**

Under the Regulations and applied GDPR, data transfers to a third country can only take place if the transfer is to an "Adequate Jurisdiction" (as specified by the EU Commission) or approval has been obtained from the ICO in respect of any measures that the data controller is proposing to take in accordance with the applied GDPR. A third country is defined as a State, territory or jurisdiction other than the Isle of Man and which is not a Member State of the European Union. The Isle of Man Parliament has approved the Data Protection (Withdrawal from the EU) (UK and Gibraltar) Regulations 2019, which enable data transfers to both territories to continue without additional safeguards post-Brexit.

**11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).**

Subject to approval from the ICO, when transferring personal data to a third country, businesses must ensure that there are appropriate safeguards on the data transfer, as prescribed by the applied GDPR.

The applied GDPR offers a number of ways to ensure compliance for international data transfers, of which one is consent of the relevant data subject. Other common options are the use of Standard Contractual Clauses or Binding Corporate Rules ("**BCRs**").

Businesses can adopt the Standard Contractual Clauses drafted by the EU Commission – these are available for transfers between controllers, and transfers between a controller (as exporter) and a processor (as importer). International data transfers may also take place on the basis of contracts agreed between the data exporter and data importer, provided that they conform to the protections outlined in the applied GDPR and have prior approval by the relevant data protection authority.

International data transfers within a group of businesses can be safeguarded by the implementation of BCRs. The BCRs will always need approval from the relevant data protection authority. Most importantly, the BCRs will need to include a mechanism to ensure they are legally binding and enforced by every member in the group of businesses. Among other things, the BCRs must set out the group structure of the businesses, the proposed data transfers and their purpose, the rights of data subjects, the mechanisms that will be implemented to ensure compliance with the GDPR, and the relevant complaints procedures.

**11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.**

Under the applied GDPR, the ICO has to approve any transfer of personal data to a third country that is not subject to an adequacy decision.

**11.4 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?**

The ICO has not published any independent advice at this time on the decision. In a news release by the ICO regarding *Schrems II*, links to the European Data Protection Board statement were provided.

**11.5 What guidance (if any) has/have the data protection authority(ies) issued in relation to the European Commission's revised Standard Contractual Clauses?**

The Isle of Man ICO has not published any independent guidance in relation to Standard Contractual Clauses.

## 12 Whistle-blower Hotlines

**12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?**

There is no reference to whistle-blowing within the data protection law or regulations. Normal standards of data protection would be expected to apply to any data processed as a result of operating such a hotline.

**12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?**

There is no reference to whistle-blowing within the data protection law or regulations and so there are no restrictions around anonymous reporting. Generally, regulatory and government guidance on whistle-blowing encourages the reporter to disclose their name to assist in appropriate action being taken.

## 13 CCTV

**13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?**

Prior approval is not required from the ICO to use CCTV. A separate notification is also not required. The ICO's guidance recommends the use of clear and visible signage, which includes who to contact about the operation of the CCTV system.

**13.2 Are there limits on the purposes for which CCTV data may be used?**

The ICO's guidance states that there must be a lawful reason for considering the use of CCTV that cannot be met in another way. The ICO also suggests that the appropriateness for use of CCTV should be kept under review. Cameras should not be installed in private areas unless there are exceptional circumstances.

## 14 Employee Monitoring

**14.1 What types of employee monitoring are permitted (if any), and in what circumstances?**

Employee monitoring is permitted, provided that compliance with the data protection legislation is achieved. Monitoring must be proportionate to the intended aim, not adversely impact the privacy of the individuals, and be justified by its benefit to the employer. It would generally be viewed as unfair to tell employees that monitoring is being undertaken for one purpose and then use the information obtained for another purpose.

**14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.**

Employers are required, on an ongoing basis, to make employees aware of any monitoring that is undertaken and the reasons for it, except in the exceptional limited circumstances where covert monitoring is necessary. Consent would only be required where an employer needed to rely on it as a legitimising condition for the processing of the personal data in accordance with the data protection legislation. Employers typically provide notice through a range of measures such as inclusion in the staff handbook, notices in the workplace and regular reminders through formal and informal communications. Employers typically obtain consent through clear and specific fair processing notices signed by the employees.

**14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?**

There is no requirement for such representatives to be notified or consulted.

## 15 Data Security and Data Breach

**15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?**

Yes. Personal data must be processed in a way that ensures security and safeguards against unauthorised or unlawful processing, accidental loss, destruction and damage of the data.

Both controllers and processors must ensure they have appropriate technical and organisational measures to meet the requirements of the data protection legislation. Depending on the security risk, this may include the encryption of personal data, the ability to ensure the ongoing confidentiality, integrity and resilience of processing systems, an ability to restore access

to data following a technical or physical incident, and a process for regularly testing and evaluating the technical and organisational measures for ensuring the security of processing.

**15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

The controller is responsible for reporting a personal data breach without undue delay (and in any case within 72 hours of first becoming aware of the breach) to the relevant data protection authority, unless the breach is unlikely to result in a risk to the rights and freedoms of the data subject(s). A processor must notify any data breach to the controller without undue delay.

The notification must include the nature of the personal data breach, including the categories and number of data subjects concerned, the name and contact details of the Data Protection Officer or relevant point of contact, the likely consequences of the breach and the measures taken to address the breach, including attempts to mitigate possible adverse effects.

**15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

Controllers have a legal requirement to communicate the breach to the data subject, without undue delay, if the breach is likely to result in a high risk to the rights and freedoms of the data subject.

The notification must include the name and contact details of the Data Protection Officer (or point of contact), the likely consequences of the breach and any measures taken to remedy or mitigate the breach.

The controller may be exempt from notifying the data subject if the risk of harm is remote (e.g., because the affected data is encrypted), the controller has taken measures to minimise the risk of harm (e.g., suspending affected accounts) or the notification requires a disproportionate effort (e.g., a public notice of the breach).

**15.4 What are the maximum penalties for data security breaches?**

The proposed revised law contains a maximum discretionary penalty of up to £1 million for breaches that are other than those prescribed in the GDPR.

## 16 Enforcement and Sanctions

**16.1 Describe the enforcement powers of the data protection authority(ies).**

(a) **Investigative Powers**:
- The ICO has powers of entry and inspection.
- Information Notice – requires a controller or processor to provide the ICO with the information that he reasonably requires.
- Through a warrant, the ICO can access all personal data, information, premises and equipment as necessary.

(b) **Corrective Powers**:
- Enforcement Notice – requires the recipient to take the steps specified in the Notice or refrain from taking the steps specified in the Notice.
- Assessment Notice – requires a controller or processor to permit the ICO to carry out an assessment of compliance with the data protection requirements.

(c) **Authorisation and Advisory Powers**: The Regulations provide the ICO with the power to issue various Codes of Practice.

(d) **Imposition of administrative fines for infringements of specified GDPR provisions**: The ICO can issue a penalty in relation to the infringement of a provision of the applied GDPR. The maximum amount for this penalty is £1 million.

(e) **Non-compliance with a data protection authority**: Failure to comply with an Information, Enforcement, Assessment or Penalty Notice may be certified to the High Court, which will treat the matter as contempt of court.

**16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?**

The Regulations entitle the ICO to impose a temporary or definitive limitation, including a ban on processing.

**16.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.**

Enforcement to date has been limited to Enforcement Notices and Formal Undertakings against Isle of Man data controllers.

**16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?**

Enforcement to date has included Penalty Notices, Enforcement Notices and Formal Undertakings against Isle of Man data controllers.

## 17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

**17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?**

The duty of confidentiality and compliance with the data protection principles would be uppermost in the minds of companies responding to such requests. Traditionally, the obligation to exchange information, such as under automatic exchange of information regimes, would be covered in an organisation's terms and conditions. For data protection reasons, though, exchange of information is often limited to Isle of Man statutory or public authorities, rather than data being released to foreign authorities. Isle of Man companies are very mindful of requests from foreign law enforcement agencies, and would be keen to ensure that these have come through the appropriate channels in advance of replying to them.

### 17.2 What guidance has/have the data protection authority(ies) issued?

There is no specific guidance in this area.

## 18 Trends and Developments

### 18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

From April 2020 onwards, the ICO has issued two Enforcement Notices and one Penalty Notice. An Enforcement Notice released in October 2020 relates to personal data breaches following a combination of poor security measures and the use of email address autocomplete. An Enforcement Notice issued in February 2021 relates to failure to comply with the right of access to personal data. A Penalty Notice imposing an administrative fine of £3,250 was issued. This Penalty Notice was issued following a complaint by a data subject in relation to their ability to exercise the right of access and the organisation's failure to comply with the data subject's request.

### 18.2 What "hot topics" are currently a focus for the data protection regulator?

The ICO is focused on publishing guidance and resources to assist data controllers and processors to comply with the Regulations and applied GDPR. The ICO has also been issuing updates in relation to measures that data controllers should take in response to COVID-19.

**Kathryn Sharman** is a trainee in DQ's Regulatory & Compliance Services Team. Kathryn advises clients on the regulatory and compliance aspects of data protection and the GDPR, with a focus on privacy notices.

**DQ Advocates Limited**
The Chambers
5 Mount Pleasant
Douglas, IM1 2PU
Isle of Man

Tel: +44 1624 632 967
Email: kathryn.sharman@dq.im
URL: www.dq.im

**Sinead O'Connor** is DQ's Head of Regulatory & Compliance Services. Sinead advises clients on the regulatory and compliance aspects of data protection. Sinead, who is a qualified data protection practitioner, regularly delivers training to Boards of Directors and senior management on the practical implications of current data protection legislation and the GDPR.

**DQ Advocates Limited**
The Chambers
5 Mount Pleasant
Douglas, IM1 2PU
Isle of Man

Tel: +44 1624 626 999
Email: sinead@dq.im
URL: www.dq.im

# Israel


Dalit Ben-Israel

Efrat Artzi

Naschitz, Brandes, Amir & Co., Advocates


## 1 Relevant Legislation and Competent Authorities

### 1.1 What is the principal data protection legislation?

The principal legislation is the Protection of Privacy Law, 5741-1981 ("**PPL**") and the Regulations enacted therefrom, the most important of which are the Privacy Protection (Data Security) Regulations, 5777-2017 ("**Security Regulations**").

### 1.2 Is there any other general legislation that impacts data protection?

The Basic Law: Human Dignity and Liberty, 5752-1992 ("**Basic Law**") impacts data protection.

### 1.3 Is there any sector-specific legislation that impacts data protection?

The Credit Data Law, 5776-2016 ("**Credit Data Law**") and certain Regulations and Rules enacted therefrom govern data protection in the credit system operated by the central bank of Israel for sharing credit data, and by the credit bureaus and business information bureaus.

The Biometric Means of Identification in Identity Documents and in an Information Database Law, 5770-2009 ("**Biometric Law**") and the Regulations promulgated therefrom govern, *inter alia*, the protection of the biometric database of Israeli citizens.

There are other sectors which are subject to additional regulatory requirements, such as the finance, insurance, medical and health sectors.

### 1.4 What authority(ies) are responsible for data protection?

The responsible authorities are:

- the Database Registrar ("**Registrar**"), which is the head of the Privacy Protection Authority (the regulatory and enforcing authority which is responsible for the protection of the privacy of individuals and for Information held in digital Databases ("**PPA**"));
- the Israel National Cyber Authority (which forms part of the Prime Minister's office), which is responsible for protecting civilian cyber space; and
- the Supervisor of Credit Data Sharing, which is responsible for data protection of credit data under the Credit Data Law.

## 2 Definitions

### 2.1 Please provide the key definitions used in the relevant legislation:

- "**Personal Data**"
  Data on the personality, marital status, intimate affairs, state of health, economic position, vocational qualifications, opinions and beliefs of an individual (defined as "**Information**"). In public entities, "Information" also includes data on an individual's private affairs. See also question 18.2 below.
- "**Processing**"
  *Inter alia*, disclosure, transfer and delivery (defined as "**Use**").
- "**Controller**"
  Whoever is responsible for all aspects associated with Databases (no formal definition, referred to as "**Owner**").
- "**Processor**"
  Whoever has a Database in its possession on a permanent basis, and is permitted to use it (defined as the "**Holder**").
- "**Data Subject**"
  The individual to whom Information contained in the Database relates (no formal definition).
- "**Sensitive Personal Data**"
  Data on the personality, intimate affairs, state of health, economic position, opinions and beliefs of an individual; Information which the Minister of Justice determined by order, following the Constitution, Law and Justice Committee of the Knesset's approval, as being sensitive information (defined as "**Sensitive Information**"). The Security Regulations include, in the first Schedule, types of data that are defined as "sensitive" (classifying the Database as having a Medium Level of Security), such as biometric, genetic, health, mental health, political opinion, religious beliefs, criminal record and communication data. In November 2018, the PPA issued a formal opinion stating that email addresses are also considered Sensitive Information.
- "**Data Breach**"
  Any incident which raises a concern as to: the integrity of the Information; unauthorised use of the Information; or use without lawful permission (defined as "**Data Breach Incidents**").
- "**Consent**"
  Informed, express or implied.
- "**Database**"
  Collection of data, kept in magnetic or optic means, which is intended for computer processing, except for: a collection of data which is designated for personal, non-commercial use; and a collection of data which only includes

names, addresses and the communication method, which in itself does not create a characterisation which violates the privacy of the individuals whose names are included therein, provided that the Owner of such collection or any entity under its control does not have another collection.

- "**Database Manager**"
  Active manager of an entity who Owns/Holds a Database, or a person who was authorised for this matter by such manager.
- "**Direct Mailing Services**"
  Enabling others to engage in direct mailing by way of transferring lists, labels or data to others by any means.
- "**Severe Data Breach Incident**"
  Any of the following: (1) in a Database with a High Level of Security – an incident of unauthorised use, or use without lawful permission, of Information from the Database, or where the integrity of the Information was compromised; (2) in a Database with a Medium Level of Security – an incident of unauthorised use, or use without lawful permission, of a material part of the Information from the Database, or where the integrity of a material part of the Information was compromised.

## 3 Territorial Scope

### 3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The PPL, as opposed to the European Union ("**EU**") General Data Protection Regulation ("**GDPR**"), does not include in its text any extraterritorial scope provisions, and generally applies to Israeli-based entities. However, according to PPA's interpretation of the PPL, in cases where there is a link between businesses established in other jurisdictions and Information of Israeli Data Subjects, the PPL may apply. For instance, where the foreign business serves as a Holder or when a foreign Owner is located abroad and collects Information of Israeli Data Subjects in connection with the provision of goods or services in Israel. There are no court precedents in this matter but there have been enforcement proceedings initiated by the PPA against foreign entities targeting affiliated companies in Israel. However, it may be difficult for the PPA to impose fines if the foreign entity does not have a local representative in Israel.

## 4 Key Principles

### 4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  The PPL (section 11) requires Owners' requests from Data Subjects to collect and use their Information to be accompanied with a notice as to: whether such Information is requested based on law or a legal requirement, or on free will; the purposes for which the Information is requested; who are the recipients of the Information; and for what purpose they will receive such Information.
- **Lawful basis for processing**
  Although the PPL does not specifically address this matter, from its overall provisions, it is concluded that the only legal basis for processing under Israeli law is Consent (express or implied), which is required in order to avoid breach of privacy (see also "**Transparency**" above).
  It can be inferred that, in specific cases, legitimate interest may be used as a basis for processing, although it has no reference in the PPL other than as a defence against claims for breach of privacy (PPL (section 18(2)(c)) (e.g., the PPA has determined that processing health data of visitors in a workplace during the COVID-19 pandemic can be justified under legitimate interest). Furthermore, Information may be processed if there is a legal, moral, social or professional obligation to do so (PPL (section 18(2)(b)). The PPL requires (in some cases) the registration of a Database with the Registrar in order to manage or possess a Database; the Registrar's guidelines (2/11) on the processing of Information by using outsourcing services ("**Outsourcing Guidelines**") prohibit the collection of Information through illegal means or use of Information which was unlawfully obtained.
- **Purpose limitation**
  The PPL (section 8(b)) prohibits the use of Information in a Database for any purpose which was not registered, and mirrors this restriction in section 11 (see "**Transparency**" above); the PPL (section 2(9)) states that using, or transferring to another, Information on an individual's private affairs otherwise than for the purpose for which it was given, without Consent, constitutes a breach of privacy. Similar provisions appear in the Credit Data Law.
- **Data minimisation**
  On March 2021, PPA issued a draft of a policy document for public consultation, regarding data minimisation ("**Minimisation Draft**"). According to the draft, the data minimisation principle is derived from the purpose limitation principle. PPA further states that Information in databases which is in excess of, and/or is not necessarily relevant for the purpose for which it was originally collected, may trigger increased occurrences of Severe Data Breach Incidents and/or potential invasion of privacy. According to the Security Regulations, Owners are obligated to annually review whether the Information stored in their database(s) exceed the information which is required for the purpose for which it was collected. Under the Minimisation Draft, PPA recommends executing such checks several times throughout the year, taking into consideration the sensitivity of the Information and the purpose for which it was collected. PPA emphasises that failure to abide by the data minimisation principle may result in breach of the Security Regulations and invasion of privacy.
- **Proportionality**
  Privacy is a constitutional right under the Basic Law (section 7), and case law extended it to data protection (see the Isakov case). The Proportionality principle was introduced in the Basic Law (section 8), and also adopted in several Registrar's guidelines, such as Registrar's guidelines (4/2012) on surveillance cameras in public areas ("**CCTV Guidelines**") and the Registrar's guidelines (5/2017) on surveillance cameras in workplaces ("**Workplace Guidelines**"), stating, generally, that the use of surveillance means should be proportionate, transparent, reasonable and fair. Such principals were also adopted in PPA's instructions (issued in 2020) regarding the implementation of the Installation of Security Cameras for the Protection of Toddlers in Day-cares Law (2018) ("**Toddlers' Security Instructions**").
- **Retention**
  - The PPL does not specifically relate to retention, but allows Data Subjects to ask for the deletion of their Information if it is inaccurate (section 14(a)). Outsourcing Guidelines allow the retention of Information with a

third-party escrow to the extent that access is required for purposes of defence against claims. The Security Regulations, Outsourcing Guidelines and clarifications issued by the PPA regarding data protection in outsourcing services ("**PPA Clarifications**") require the deletion of Information upon termination of the agreement(s) between Owner and service provider(s). See also "Data Minimisation" above.

- The Credit Law includes specific retention periods for the credit data in the national repository.
- The Registrar's guidelines (2/2012) on recruiting activities ("**Recruiting Guidelines**") require employers and placement services to destroy or anonymise candidates' Information immediately when their use of it is complete (employers may maintain opinions in an archive for lawful purposes, on a "need-to-know" access basis, and keep a copy in the employee's personal file).

## 5 Individual Rights

### 5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**
  The PPL (section 13(a)) entitles Data Subjects to inspect their Information which is stored in the Owner's Database. This right was extended in case law to obtaining a copy of such Information, and a Registrar's guideline (1/2017) further extended it to any format (including video, text messages and voice recordings). There are some exceptions, such as: physical or mental health; violation of legal privilege; investigations and law enforcement, etc. See also "**CCTV**" below.
- **Right to rectification of errors**
  The PPL (section 14(a)) entitles Data Subjects to submit a request to the Owner (or Holder if the Owner is a non-resident) to amend or delete his/her Information if it is incorrect, incomplete, unclear or outdated. The Owner will inform the Data Subjects as to whether it agrees to or refuses such request: the Holder will comply with the Owner's agreement to amend the Information and/or as instructed by court order. The Owner's refusal entitles the Data Subject to appeal to the competent court.
- **Right to deletion/right to be forgotten**
  See the previous section, and "**Data Minimisation**" above. Further, the PPL (section 17F(b)) entitles the Data Subject to be deleted from a Database used for Direct Mailing. The Registrar's guidelines (2/2017) expand such right to databases for Direct Mailing Services, stating that when the Database is being used for additional purposes, deletion is limited only to the Direct Mailing list. The Biometric Law includes provisions for deletion (adults and minors under the age of 16). The Credit Data Law entitles an individual who believes that the Information about him/her is incorrect, incomplete or inaccurate to request from the Bank of Israel the deletion, completion or rectification of the Information.
- **Right to object to processing**
  The PPL does not address this right specifically, but in some cases Data Subjects can withdraw their Consent. See also "**Marketing**" below. The Biometric Law includes provisions regarding this right (adults and minors under the age of 16).
- **Right to restrict processing**
  See above.
- **Right to data portability**
  The PPA and the Consumer Protection and Fair Trade Authority (the Israeli governmental authority established by the Consumer Protection Law, 5741-1981), issued on January, 2021, a joint draft of a proposed policy for public consultation, elaborating the main principles required for incorporating a principle of data portability as an integral part of Data Subjects' rights (the "**Portability Draft**"), similarly to the principles under Article 20 to the GDPR and the CCPA. The Portability Draft generally states that certain organisations (whose characteristics have not yet been determined) will be required to grant their customers/consumers a general data portability right; such right shall apply only to digital Information and will be free of charge; the transfer of Information will be secured, and the Information will be transferred online, in a readable format. Specific sectors may be subject to additional specific regulations.
- **Right to withdraw consent**
  See "Right to object Processing".
- **Right to object to marketing**
  See section 9 below.
- **Right to complain to the relevant data protection authority(ies)**
  Not applicable under the PPL. A Data Subject can appeal or file a claim to a competent court. Furthermore, as an integral part of its enforcement activity, the PPA enables complaints to be raised via its website.

## 6 Registration Formalities and Prior Approval

### 6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

Subject to certain exemptions, a Database must be registered with the Registrar if it contains: Information about more than 10,000 individuals; Sensitive Information; Information about individuals which was not provided by them, on their behalf or with their Consent; Information which belongs to a public entity; and/or Information which is used for Direct Mailing Services. Processing activities should be described in the application.

### 6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

The application must be specific, completed in its entirety, and the processing activities and all other information should be detailed.

### 6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

Registrations and notifications are made per legal entity's Database (which can be a number of IT systems forming a legal Database), and per purpose for Use of the Information (which may differ between Data Subject categories).

**6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?**

Registration applies to Owners. The PPL does not specifically address applicability to Israeli citizens, residents or territoriality; however, the PPA's position is – and case law implies – that the registration obligation applies to Israeli Data Subjects, regardless of where the Information is collected, stored or processed.

**6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?**

The following Information must be included: the Owner's details; whether the Owner is a bank, insurance company or deals with rating and evaluating credit; the number of Data Subjects and people who are authorised to access the Database; the Database's technical infrastructure; types of Information included in the Database; purpose(s) for Use; how the Owner received such Information (directly from the Data Subject or otherwise); the Database Manager's details; and the Holder's details and purposes for Use of the Information by the Holder.

**6.6 What are the sanctions for failure to register/notify where required?**

It is a criminal offence which is punished with one year's imprisonment and the imposition of administrative fines (up to 2,000 NIS for individuals and 10,000 NIS for corporations). The PPA does not enforce the registration obligation if the material obligations under the PPL and Regulations have been complied with. There are no precedents for imposing fines or criminal liability for lack of registration.

**6.7 What is the fee per registration/notification (if applicable)?**

This is not applicable.

**6.8 How frequently must registrations/notifications be renewed (if applicable)?**

In case of changes in the Information previously reported (PPL (section 9(d)). When a Database is no longer used, it has to be deleted and reported to the Registrar.

**6.9 Is any prior approval required from the data protection regulator?**

The Registrar's approval of the registration form request is mandatory in order to be able to use the Database. However, an Owner can use the Database when no response was provided within 90 days following the submission for registration.

**6.10 Can the registration/notification be completed online?**

Yes, registration and updating requests can be completed online.

**6.11 Is there a publicly available list of completed registrations/notifications?**

No, but there is an online registry which presents partial information from the registered Database forms.

**6.12 How long does a typical registration/notification process take?**

Between a few days and several weeks.

## 7 Appointment of a Data Protection Officer

**7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.**

The PPL (section 17B) requires the appointment of a Data Security Officer (whose duties are partially similar to the Data Protection Officer under the GDPR) ("**Security Officer**") in the following circumstances: Holder of five Databases that require registration; public body; bank; insurance company; or company involved in rating or evaluating credit. In the Outsourcing Guidelines, PPA recommended that both Owner and Holder will appoint a Security Officer when processing Information through outsourcing services. The Biometric Law (section 26) mandates the appointment of a Security Officer for the biometric Database.

In 2020, PPA issued draft recommendations for public consultation, recommending organisations to appointment with the Data Privacy Officer ("**DPO**"), (such appointment is not applicable under the PPL, but is required under the Credit Data Law (section 18)), *inter alia*, for the purposes of raising awareness within the organisation to the right for privacy and improving compliance for the PPL and the Regulations enacted therefrom (the "**DPO Draft**"). The PPA has since been promoting these draft recommendations as a best practice.

**7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?**

Failure to appoint a Security Officer is a criminal offence which is punished with one year's imprisonment and the imposition of administrative fines (up to 3,000 NIS for individuals and 15,000 NIS for corporations).

**7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?**

No. However, in contrast to a Database Manager, a Security Officer does not assume personal liability.

**7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?**

Yes, provided that it does not constitute a conflict of interest with the Security Officer's other duties. In addition, the Security Officer has to be subject to the authority of each Database Manager in relation to that Database, and according to the DPO

Draft, PPA elaborates that the Security Officer should comply with the DPO's professional instructions regarding the implementation of security measures.

**7.5 Please describe any specific qualifications for the Data Protection Officer required by law.**

The PPL (section 17B) requires the Security Officer to be competent and qualified, and not to have been convicted of an offence involving moral turpitude or the PPL's provisions. The Security Regulations (section 3) stipulate that the Security Officer shall report directly to the Database Manager or to the Owner/Holder's active manager (as applicable), or to another senior officer who directly reports to the Database Manager. The DPO draft requires that a DPO who is also performing another role will not be in a conflict of interest and his/her qualifications include: academic studies in law; accounting; IT or regulation; deep knowledge of Israeli data protection laws; understanding of IT and information security; familiarisation with the business aspects of the organisation; and professional ethics.

**7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?**

The Security Officer is responsible for the security of the Information stored in the Database (PPL (section 17B(b)). The Security Regulations (section 3) add the following duties: preparation of a data security procedure and a plan for regular monitoring of compliance with the Security Regulations and reporting its findings to the Owner and Database Manager. Under the DPO Draft, PPA emphasises that the Security Officer is also required to ensure compliance with security standards and procedures, in order to prevent unlawful use of the Information. The responsibilities of the DPO under the DPO draft include: drafting the privacy policy; being involved in all data processing activities; privacy by design and by default; compliance of procedures with privacy laws; performance of DPIAs; DSARs and complaints handling; audits and reporting obligations; and training.

**7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?**

For the Security Officer – yes, annually. For the DPO – under the DPO draft – no.

**7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?**

See above.

## 8 Appointment of Processors

**8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?**

Yes. The Owner is required to enter into an agreement with each Holder or third party who has access to the Information (Security Regulations, section 15). Similar obligations exist in the Outsourcing Guidelines, PPA Clarifications, and the guidelines that apply to the finance, banking and insurance sectors.

**8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?**

The Security Regulations, Outsourcing Guidelines and PPA Clarifications require the following main issues to be addressed: the Information which the service provider may use, the systems it may access and the permitted processing activities; the duration of the agreement and the manner of returning and deleting the Information; security instructions; procuring the signature of the service provider's authorised users on confidentiality undertakings, data protection and the limited purpose of use of the Information; and service provider's obligations with respect to its sub-contractors, provision of compliance reports, and reports of Data Breach Incidents.

## 9 Marketing

**9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).**

The PPL defines "Direct Mailing" as contacting a person where he/she belongs to a group which is classified by one or more shared characteristics of the individuals who are included in a Database. Direct Mailing can be sent in any media, and may be of a promotional nature. Each Direct Mailing must state the following: it is a Direct Mailing message; the registration number of the Database used for the Direct Mailing Services; the Owner's identity and address; and the sources from which it received the Data Subject's details. If the Information was provided by the Data Subject, the PPA recommends indicating the circumstances under which it was provided, allowing the Data Subject to opt out, and incorporating an "unsubscribe" option. According to the Registrar's guideline (2/2017), if Direct Mailing is being used for offering services and/or products which are related to the Owner's main activity, in a standard-form contact, the Owner should allow the Data Subject to opt out, even if it results in the inability to receive the services. Databases for purposes of Direct Mailing are subjected to duties towards the Data Subject regarding notice, access, rectification and deletion.

The Communications Law (Telecommunications and Broadcasts), 5742-1982 ("**Spam Law**") defines "Spam" as automated messages sent electronically (through email, SMS, fax, or automatic dialling system) to an unknown recipient list, mainly for marketing and promotional purposes. Except for exemptions, sending Spam requires the recipient's opt-in Consent. When the exemptions apply, opt-out is sufficient. The header of Spam messages needs to include the words "advertisement", "marketing email" or a similar term. All Spam communications must state the full name, address and contact details of the entity sending the communications.

**9.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?**

The Direct Mailing restrictions apply to communications sent to individuals; therefore, if they are sent to business emails not associated with an individual (e.g. office@XX.co.il) they will not fall under the PPL's restrictions. However, communications

to business email addresses that belong to a specific individual (i.e. john.smith@XX.co.il) will be subject to the PPL Direct Mailing restrictions. The Spam Law restrictions apply to all marketing communications, including business-to-business, with the exception of a one-time approach to a recipient that is a business, in which the business is requested to approve the receipt of Spam.

**9.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).**

Marketing activity not covered under the Spam Law, i.e. through human phone calls or post, will not be considered as Spam and there are no special requirements, unless the activity is considered "Direct Mailing" (i.e. sent to a specific targeted audience).

**9.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?**

As mentioned in section 3 above, if the Owner is located abroad and collects Israeli Data Subjects' Information in connection with the provision of goods or services in Israel, then the PPL applies. Therefore, at least in relation to Direct Mailing targeting Israeli Data Subjects in connection with the provision of goods or services in Israel, as opposed to the Spam Law, the restrictions may apply.

**9.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?**

The PPA enforces breaches of Direct Mailing and Direct Mailing Services; claims for sending Spam are not under the PPA's authority and are mostly subject to private claims and class actions.

**9.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?**

Yes, subject to certain recommendations issued by the PPA: the purchaser will receive the seller's written confirmation that its activities are legal, and that it fully complies with PPL requirements; the seller duly registered a Database, lawfully collected the Information, and maintains a list indicating the source from which the Information was acquired, and the identity of the person/persons or an entity/entities to whom/which the Information was sold; the Database's name should be examined; the Database's purposes should include Direct Mailing Services, and the sale of Information matches the uses requested by the purchaser; and the seller duly received the Data Subject's Consent for such purposes.

**9.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?**

For sending Direct Mailing from a Database for Direct Mailing, there are administrative fines (up to 3,000 NIS for individuals and 15,000 NIS for corporations). For Spam, there are statutory damages of 1,000 NIS (without proving actual damages) and a possible class action.

## 10 Cookies

**10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).**

There are no restrictions under the PPL and the Regulations. In April, 2021, following the receipt of public comments, PPA issued recommendations regarding certain privacy-related issues in the scope of using advance technological tools/applications for payment transfer (such as mobile/digital wallets), and stated, inter alia, that operators of mobile/digital wallets should receive opt-in consent to use cookies when a customer/consumer uses their mobile/digital wallets, and incorporate a separate, detailed explanation regarding the implications of the collection and use of Information through cookies. In 2017, the PPA has already issued recommendations for businesses operating websites/applications for online trading which, *inter alia*, require that website/application's privacy policy to indicate whether the website/application contains technological tools for tracing users (such as cookies) and the purpose of their use.

**10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?**

No, there is no distinguishing between different types of cookies.

**10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?**

Not that we are aware of.

**10.4 What are the maximum penalties for breaches of applicable cookie restrictions?**

This is not applicable.

## 11 Restrictions on International Data Transfers

**11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.**

The Protection of Privacy (Transfer of Data to Databases Abroad) Regulations, 5761-2001 ("**Transfer Regulations**") restrict the ability to transfer Information abroad, unless the law of the country to which the Information is being transferred ensures a level of protection no less than that provided under Israeli law, or to the extent any of the exemptions set forth in the Transfer Regulations are met (for example: the Data Subject Consented; Information is transferred to a corporation under the control of the transferring Owner and the recipient guaranteed the protection of privacy after the transfer; transfer to an entity which contractually undertakes to comply with Israeli law; and transfer to a country which is a party to the European Convention for the Protection of Individuals with Regard to Automatic Processing of Sensitive Data). When transferring Information abroad, the Owner should ensure, in a written agreement, that the recipient takes adequate measures to ensure the privacy of the Data Subjects and guarantees that the Information shall not be further transferred.

**11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).**

The most common mechanism, especially when Information is transferred to cloud service providers, is to use Regulation 2(8) of the Transfer Regulations, which allows the transfer to an EU country or the UK (see question 11.4 below), or to receive the recipient's contractual obligation to comply with the requirements of Israeli law *mutatis mutandis*, or to receive the Data Subject's Consent (which is typically done through a published privacy policy since Consent can be implied).

**11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.**

The Owner is required to indicate in the registration form whether the Information is being transferred to a third party (whether in Israel or abroad).

**11.4 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?**

In 2020, the PPA issued an opinion, clarifying that although the United Kingdom is no longer a member of the European Union, the transfer of Israeli Data Subjects' Information to the UK is still permissible under Regulation 2(8)(1) to the Transfer Regulation, as the UK previously signed the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108).

Following the CJEU decision on the invalidation of the Privacy Shield Framework, the PPA has repeated its former opinion (issued in 2015, following the cancellation of the Safe Harbor agreement) regarding the use of Regulation 2(8)(2) of the Transfer Regulations as a mechanism to transfer personal information of Israeli data subjects to the USA, and announced that transfer of Information to the USA can no longer rely on the EU-U.S. Privacy Shield or on the determination that the US is an adequate country in terms of Israeli law, and may only be permissible by using the other remaining mechanisms in the Transfer Regulations.

**11.5 What guidance (if any) has/have the data protection authority(ies) issued in relation to the European Commission's revised Standard Contractual Clauses?**

None, as the Standard Contractual Clauses are not considered by the PPA as an applicable mechanism for the transfer of Information from Israel, abroad.

## 12 Whistle-blower Hotlines

**12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?**

This is not applicable in Israel.

**12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?**

No, anonymous reporting is not prohibited.

## 13 CCTV

**13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?**

Footage of Data Subjects from CCTV cameras qualifies as a Database that requires registration. A registration form for CCTV cameras shall include, in addition to the details set forth in question 6.5 above, a detailed query about the implementation of the CCTV Guidelines and the Workplace Guidelines, whichever is relevant for the registration. For PPA approval, see question 6.9 above.

In order to comply with PPL (section 11) provisions, the CCTV Guidelines require a clear, legible sign to be posted both at the entrance to the location of the cameras and in the area covered by the cameras. The sign should include an image, the name of the entity installing the cameras, the purpose (e.g., "theft prevention", "safety and security", etc.) and a reference to where the full policy for the use of CCTV cameras can be accessed (website) or contact details for additional information.

**13.2 Are there limits on the purposes for which CCTV data may be used?**

Due to the significance of the right to privacy, the CCTV Guidelines require installation and use of CCTV cameras to be evaluated against less invasive alternatives, and that their use achieves proper and limited purpose(s). The use of the CCTV cameras' footage is allowed only for the purpose(s) for which the Owner received Consent from the Data Subject. There are additional limitations for use of CCTV cameras in public areas frequented by minors, facial recognition, where CCTV footage is matched with other Information in a Database, and when CCTV cameras are used in the workplace.

## 14 Employee Monitoring

**14.1 What types of employee monitoring are permitted (if any), and in what circumstances?**

Case law and the Registrar's guidelines permit limited and narrow monitoring of employees, subject to certain limitations.

In 2011, the *Isakov* case (Labour Appeal 90/08, *Tali Isakov Inbar v. Commissioner for Women's Labour*) imposed restrictions

on the ability to monitor employees' emails and usage of the workplace computer systems, by differentiating between professional, external personal, and dual email accounts. Whereas a professional account (which is intended only for work communications) may be subject to monitoring, surveillance and backup (however, personal emails, to the extent they exist, may be accessed only subject to the employee's explicit, informed and freely given Consent, and only if the personal messages are unlawful or abusive), an external personal account (the employee's private email account) may not be monitored except by a court order, and personal emails in a dual account (used for both personal and work purposes) may be monitored only if: unusual circumstances that justify access to the messages exist; less invasive tools are used first; there is explicit, informed and freely given Consent to the corporate email policy and, specifically, to the monitoring of or access to the employee's personal messages; or the employee provides specific Consent to each access or surveillance activity by the employer that includes the personal content of the account.

The Workplace Guidelines stipulate that installation of surveillance means in the workplace is allowed only for legitimate purposes which are essential to the employers' interests, in accordance with the employers' business agenda or when it is required to fulfil a legal obligation. The employer is required to establish a clear, detailed policy for the use of CCTV cameras, to be presented to the employees (and, where applicable, be subject to approval by the employees' representatives or unions). The Policy will, *inter alia*, include the extent and purposes of the use of CCTV cameras, the places where the cameras are installed (subject to specific justifications required for the installation of surveillance means in certain sensitive areas) and the employees' rights.

In the Toddlers' Security Instructions, PPA tried to balance between the employees' (and the toddlers') rights for privacy, and the necessity to protect toddlers throughout their stay at the daycare, and, *inter alia*, stated that the cameras should be visible, cannot be installed in private areas and/or record audio, the photos will be retained for no more than 30 days, and the access to them should be limited.

In 2017, the National Labour Court ruled that using biometric time clocks for work presence monitoring (collecting fingerprint biometric Information) is illegal, since less invasive measures are available (Labour Case 7541-04-14, *The Employees Union v. Kalansua Municipality*, and others). The court ruled that collection and storage of fingerprints infringes an employee's privacy and autonomy, which are both constitutional rights, and is unbalanced against the risks of misuse or unauthorised use for purposes beyond those originally intended. The court concluded that employers may not require employees to provide fingerprints, or any other biometric information, unless a statute expressly permitting it is enacted or if the employee provides specific, freely given Consent.

**14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.**

Consent is required to avoid violation of privacy under the PPL; however, due to the unbalanced employer-employee relationship, case law has determined that employees' Consent needs to be explicit, informed and freely given. Consent may be obtained through the employment agreement or through the corporate policies which are made available to the employees, and they are required to confirm that they have read them.

According to the Isakov case, the employer needs to implement a policy for the use of corporate IT systems and email accounts, notify the employees of the policy and incorporate it into the employees' employment contracts. This is usually an integral part of the employment contract, or a separate document which is brought to the attention of the employees by a notice in the employment contract, intranet or otherwise. Monitoring employees' personal email is subject to their specific, explicit, informed and freely given Consent.

The Workplace Guidelines require explicit, informed and freely given Consent for installing CCTV cameras in the personal office or private workspace of the employee; as opposed to the public areas of the workplace, in which notification is sufficient. According to the Toddlers' Security Instructions, the employer needs to inform each employee, prior to the effective date of his/her employment, orally and in writing, about the existence of cameras, the purpose for their use, their locations and limitations regarding the access and use of the footage.

Recruiting Guidelines state that if, on or before the day on which the candidate was tested, he/she gave Consent to additional use of his/her Information (meaning for purposes exceeding completion of the recruitment procedures for the specific position), it shall be deemed as Consent given without free choice and therefore invalid. The candidate's Consent is likely to be valid only if it was given after the candidate's acceptance or rejection of the position for which he/she was originally tested.

**14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?**

General case law requires consultation with unions when employee rights may be affected, and certain collective bargaining agreements, if applicable, may require notification or consultation in specific cases. See also question 14.1 above.

## 15 Data Security and Data Breach

**15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?**

The PPL (section 17) imposes security obligations on the Owner, Processor and Database Manager. The Security Regulations specify the security measures which need to be implemented, based on the security level of each Database.

**15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

The Security Regulations (section 11(d)) require a Severe Data Breach to be reported to the Registrar immediately, including the measures taken to mitigate it. The report should, *inter alia*, include the date of the incident and any detail associated therewith, a description of the security measures, the Information which was affected, potential implications on the respective Data Subjects which were included in the affected Database, and what actions were taken to protect the Information.

The PPA clarified in guidelines issued that "immediately" means within 24 hours from the occurrence of the incident, and no later than 72 hours. Also, although the reporting obligation applies to Owner, Processor and Database Manager, the PPA

explained that a single report is sufficient in order to comply with the reporting obligation.

**15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

No, unless otherwise instructed by the Registrar (following consultation with the national cyber directorate) and based on the assessment of the implications of the breach on data subjects.

**15.4 What are the maximum penalties for data security breaches?**

As of July 2019, data security breaches are enforced by the PPA as an integral part of its authority. See question 16.1 below.

## 16 Enforcement and Sanctions

**16.1 Describe the enforcement powers of the data protection authority(ies).**

(a) **Investigative Powers**: PPA has the authority to open criminal and administrative investigations (including sectorial enforcement proceedings), to enter into premises, search and seize materials and objects.
(b) **Corrective Powers**: PPA has the authority to instruct the repair of violations.
(c) **Authorisation and Advisory Powers**: Under certain circumstances, PPA may issue a preliminary opinion regarding the interpretation of the PPL and the Regulations. Other than that, this is not applicable in Israel.
(d) **Imposition of administrative fines for infringements of specified GDPR provisions**: According to the Administrative Offences Regulations (Administrative Fine – Protection of Privacy) 2004, a breach of PPL (section 31A) may, *inter alia*, impose administrative fines upon individuals (2,000–5,000 NIS), and five-fold for corporations, and for continuing violations, one-tenth of the fine for each day of the violation.
(e) **Non-compliance with a data protection authority**: PPL states (section 10(f) that non-compliance with the Registrar's instructions may result in suspension or cancellation of the Database's registration. In addition, as PPA's guidelines are binding – breach of the PPA's guidelines may be considered a breach of certain provisions of the PPL and/or Regulations, and impose civil and/or administrative sanctions. See also question 16.1(a) and (b) above.

**16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?**

Yes, if the processing activity is illegal or otherwise not aligned with the PPL or the Regulations. A court order is not required.

**16.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.**

In May, 2021, PPA completed a criminal investigation (in collaboration with the Israel police) regarding the unauthorised access to Sensitive Information which was stored in certain insurance companies, the national insurance institute of Israel and other companies' databases. Such unauthorised access was made by private investigators, who deceptively obtained identifying information about individuals from illegal source(s), used it in order to impersonate to such individuals, and mislead the employees of the aforementioned bodies/companies in order to gain access to such individuals' economic and/or other Sensitive Information. PPA handed over its findings to the prosecutor, for its decision.

In May 2021, PPA stated that Hod-Hasharon municipality breached the PPL and the Regulations enacted therefrom, due to a Severe Data Breach Incident which was reported by the municipality. PPA concluded that although Information and/or Sensitive Information about Hod-Hasharon's residents and/or the municipality's employees were not leaked, it was accessible to unauthorised users. PPA instructed to repair the security violations, and also imposed an administrative fine of 10,000 NIS on the municipality, for not registering a database as legally required.

In January, 2021, PPA stated that the "Likud" and "Israel Beiteinu" parties (who participated in the 23rd election in Israel, during March 2020) and Elector Software Ltd ("**Elector**"), a company which developed a designated application containing the entire Israeli voter's registry which was used by such parties, are liable as an Owner and Holder of Database (respectively), for breach of the PPL and the Regulations enacted therefrom, due to leakage of the entire Israeli voter's registry from the application. PPA, *inter alia*, revealed severe data protection impairments in the application, unlawful use of former voter's registrar and other violations. PPA instructed the repair of the violations, declared a breach of the PPL and the Regulations (and published it on the PPA's website), and also imposed administrative fines on Elector (the amount of which was not published).

In June 2020, PPA completed a criminal investigation against a flight attendant of an airline who provided his identification details and IT passwords to an employee of a vendor, and such details enabled the latter to review the personal information of other flight attendants and thousands of the airline's passengers, including details regarding disabilities. PPA's findings were transferred to the State Attorney's office for their decision on criminal proceeding against the individual.

See also question 18.1 regarding the enforcement proceedings executed by the PPA during 2020 and 2021.

**16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?**

See question 3.1 above.

## 17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

**17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?**

There are no specific rules. The practice is to comply with the request based on the rules in the requesting country, considering the need to comply with Israeli privacy laws and trans-border data limitations. The Legal Assistance between Countries Law, 1998 stipulates that the Minister of Justice may approve

legal assistance to another country, *inter alia*, through disclosure of documents and information, if the request is submitted by a competent authority in the requesting country. If there are cross-border restrictions in relation to e-discovery, the practice is to obtain contractual and information security safeguards from the party performing the discovery process.

### 17.2 What guidance has/have the data protection authority(ies) issued?

This is not applicable.

## 18 Trends and Developments

### 18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

During 2020 and 2021, PPA continued executing enforcement proceedings in order to evaluate the level of compliance with the PPL and the Security Regulations, increase awareness of the PPL and Security Regulations' provisions, and detect sectorial or other failures that require the PPA's intervention or issuance of specific guidelines. The enforcement proceedings, *inter alia*, covered the following sectors/topics: medical institutes and laboratories; mental health medical centers; companies that provide storage and hosting services; political parties who participated in the 23rd elections in Israel and entities that assist individuals in obtaining and executing their medical rights. The major areas of non-compliance are in implementation of appropriate security measures and policies, non-compliance with the provisions of the PPL (including failure to register a Database, delete a Database which is no longer in use, and protecting Data Subject's rights). See also question 16.3 above.

### 18.2 What "hot topics" are currently a focus for the data protection regulator?

As stated above, the PPA has been active in publishing various drafts of policy papers on the following matters: DPO appointment, data minimisation, data portability and PPA's interpretation for the term Information (see below). All of the foregoing are still in a draft status and final versions have not yet been published. Additional recommendations published by the PPA regarding privacy-related issues pertaining to the use of mobile payment and wallet applications, and on "strong" passwords. There have been attempts in the past year to introduce amendments to the PPL by a draft proposed bill to amend certain definitions and align them to GDPR and cancel the database registration obligation on certain cases and a draft bill that was reintroduced on enforcement powers of the PPA. These legislative actions have not progressed due to the political situation in Israel and recent elections, and this may be the reason for the PPA to issue on May, 2021, a draft for the public consultation, containing its interpretation to the term "Information" and "information about an individual's private affairs" (which is used in the PPL, but it is not defined), based on case law ("**Information Draft**"). In the Information Draft, PPA clarifies that although the term "Information" is defined narrowly under the PPL, it should be interpreted to include information about a person which can be identified by using reasonable means, and information from which a reasonable person can infer on individual's affairs and traits (as included in the current definition of "**Information**"); the types of information which are included in "Information about an individual" will be interpreted on a case-by-case basis, in order to protect the individual's right for privacy.

The PPA has issued several guidelines and recommendations in relation to the COVID-19 pandemic, the most important one regarding personal data collection through epidemiological investigations conducted to detect contacts with affected individuals.

During the pandemic, the ministry of health in Israel used a technological tool developed by the Israeli Security Agency ("**ISA**") as a means for contact tracing. Such use was subject to several petitions before the High Court of Justice. As a result of the High Court of Justice ruling on May 4, 2020, specific primary legislation was adopted enabling the continued authority of the ISA to collect technological data in order to fight the pandemic. This law was enacted for a limited term and required an announcement by the government that the continued use is required and there are no alternative civilian means. On March 1, 2021, the High Court of Justice determined that due to the status of the pandemic and the high vaccination rate, if ISA is still required to assist in providing technological data, the government must define a set of objective transparent criteria and use ISA only as a supplementary tool in cases when an infected individual is not cooperating with the epidemiological investigation or refuses to disclose his/her contacts. As a consequence, criteria were defined but as of March 29, 2021, the foreign affairs and defence committee of the parliament decided not to approve the amended government's declaration on the continued assistance of ISA.

The current hot topic is a collection of information about vaccination and recovery from COVID-19, both by employers and businesses. There are specific regulations in relation to entering public places, such as restaurants, gyms and locations in which performances or events are taking place. There are specific regulations regarding dining rooms and sport activities at workplaces and recent legislation enabling collection of this information by public sector employers. Other than that, there are no general guidelines on the subject.

**Dalit Ben-Israel** is an expert in the fields of Computer, Information Technology, Cyber, Privacy and Data Protection Law. Dalit has vast expertise in privacy, which encompasses regulatory compliance including Israeli law, GDPR and CCPA, assistance to clients in regulator audits and enforcement actions, drafting and negotiating a variety of cloud and data processing agreements, web and application terms of use, privacy statements, drafting and reviewing data security policies and procedures, handling data breach cases and security incident management, spam issues, and counselling insurance companies on cyber insurance coverage; rendering cybersecurity and regulatory consulting in these areas to diverse clients, *inter alia*, in the financial and insurance sector. Dalit writes posts and articles on her areas of expertise, lectures and provides training on Israeli and GDPR compliance issues. Dalit is a member of IAPP – the International Association of Privacy Professionals, and during 2019–2020 she served as the co-chair for the Israeli KnowlegeNet chapter of IAPP.

**Naschitz, Brandes, Amir & Co., Advocates**
5 Tuval Street
Tel-Aviv 6789717
Israel

Tel: +972 3 623 6010
Email: dbenisrael@nblaw.com
URL: www.nblaw.com

**Efrat Artzi** specialises in Computer, Information Technology, Cyber, Privacy and Data Protection Law. During the course of her work, Efrat provides legal consultation to the firm's clients in diverse aspects of privacy law, compliance and data protection (under Israeli law, GDPR and CCPA); has vast experience in drafting web and application terms of use, privacy policies and privacy notices, data processing addendums, and data protection policies and procedures; and extensively interacts with the Israeli Privacy Protection Authority. Efrat also handles various commercial contracts, especially in information technology transactions (including computerisation projects, cloud and SaaS service agreements, etc.), and provides overall comprehensive legal support to the firm's clients in extensive areas, on their ongoing activities. Efrat is a member of the IAPP – the International Association of Privacy Professionals.

**Naschitz, Brandes, Amir & Co., Advocates**
5 Tuval Street
Tel-Aviv 6789717
Israel

Tel: +972 3 623 6070
Email: eartzi@nblaw.com
URL: www.nblaw.com

Naschitz, Brandes, Amir is one of the leading law firms in Israel with over 200 legal professionals. We have been a market leader for many years and are a first port of call for domestic and international clients. From emerging companies to market leaders, our clients span a broad range of industries, including hi-tech, financial services, insurance, bio-med and others.

Our Data Protection Practice provides comprehensive counselling and guidance on all aspects of privacy, data protection and cyber security. We devise creative and practical solutions based on in-depth understanding of cyber and security threats. We counsel on a full range of matters, including drafting and negotiating agreements and policies and providing ongoing counselling.

Our services are focused on assisting our clients in the various stages of compliance and implementation of local and foreign regulations, with the current focus on the GDPR and CCPA, as well as assistance in audits and enforcement actions.

**www.nblaw.com**

נשיץ ברנדס אמיר
NASCHITZ BRANDES AMIR

# Japan


Hiromi Hayashi


Masaki Yukawa

Mori Hamada & Matsumoto



## 1 Relevant Legislation and Competent Authorities

### 1.1 What is the principal data protection legislation?

The following laws and regulations have been the basic legislation in Japan for the protection of Personal Information since 2005:

(i) Act on the Protection of Personal Information (Act No. 57 of May 30, 2003, as amended; the "**APPI**");

(ii) Act on the Protection of Personal Information Held by Administrative Organs (Act No. 95 of 1988 of May 30, 2003, as amended);

(iii) Act on the Protection of Personal Information Held by Independent Administrative Agencies; and

(iv) local regulations (*jyourei*) legislated by local governments.

The Personal Information Protection Committee (the "**PPC**"), which is the main agency that supervises the enforcement and application of the APPI, issues general guidelines on the implementation of the APPI. There are also other guidelines for specific sectors issued by other ministries.

An amendment to uniformly apply the APPI to both the public sector and the private sector by (i) abolishing the Act on the Protection of Personal Information Held by Administrative Organs and the Act on the Protection of Personal Information Held by Independent Administrative Agencies, and (ii) introducing requirements applicable to local governments, subject to adjustments by local regulations to the extent consistent with the APPI (the "**2021 Amendment**") was promulgated in May 2021. The amendments with regard to the public sector, excluding local governments, will be enforced by May 2022 and the amendments with regard to local governments will be enforced by May 2023.

Prior to the 2021 Amendment, another amendment to the APPI was promulgated in June 2020 and will take effect in April 2022 (the "**2020 Amendment**"), although the increased maximum penalties have already taken effect since December 2020 and a transition clause will take effect in October 2021. Under the transition clause, notifications to affected data subjects and the PPC under the strengthened requirements for third-party provision of personal data, which requirements will take effect in April 2022, can be made in advance for a smooth transition.

**APPI**

The APPI is the principal data protection legislation. It is the APPI's basic principle that the cautious handling of Personal Information, as defined in Article 2, paragraph 1, under the principle of respect for individuals, will promote the proper handling of Personal Information (APPI, Article 3).

Chapters 2 and 3 set forth the basic frameworks of the responsibilities and policies of the national and local governments to protect Personal Information. Pursuant to Article 7 of the APPI, the Cabinet established the "Basic Policy on the Protection of Personal Information" (*Kojin Jyouhou no Hogo ni kansuru Kihon Houshin*) in 2004 (as amended; the "**Basic Policy**").

Chapter 4 regulates the use of Personal Information by private businesses and sets forth the obligations of "Business Operators Handling Personal Information" (*Kojin Joho Toriatsukai Jigyosha*) (the "**Handling Operators**"), as defined in Article 2, paragraph 5 of the APPI. Any business operator using a Personal Information Database (please see question 2.1) is considered a Handling Operator regardless of the scale of its Personal Information Database (the exemption granted to small business operators with a Personal Information Database of fewer than 5,000 individuals was abolished on May 30, 2017). The handling of data by administrative organs and independent administrative agencies is regulated under the laws described in items (ii) and (iii) of the laws listed in the first paragraph above until the 2021 Amendment takes effect.

**Privacy Mark**

A business operator may use a logo called a "Privacy Mark" (the "**Privacy Mark System**") which shows its compliance with the relevant laws and the Japan Industrial Standards (JIS Q 15001:2017 [Personal Information Protection Management System – Requirements]) ("**JIS Q 15001**") established by the Japan Information Processing Development Center. JIS Q 15001 is not a law but, in certain aspects, it provides a higher level of standards than the APPI.

### 1.2 Is there any other general legislation that impacts data protection?

(a) **Privacy Right**

The privacy right is recognised by Japanese courts as an individual's right to keep their private life not to be disclosed without a legitimate reason, and is recognised among academics as the right to control one's own Personal Information. Therefore, in addition to complying with the APPI, a person who possesses the Personal Information of others in Japan must not infringe on the privacy rights of the principals.

(b) **Privacy of Communications**

Article 4 of the Telecommunications Business Law provides that no person may infringe on the privacy of the communications handled by telecommunications business operators. Privacy of communications does not necessarily refer to Personal Information, although the guidelines issued

by the Ministry of Internal Affairs and Communication ("**MIC**") for the protection of Personal Information in the telecommunication business (please see question 1.3) also deal with the privacy of communications, such as telecommunications logs (the "**MIC Guidelines**").

(c) **Electronic Mail**
The Act on the Regulation of Transmission of Specified Electronic Mail (Act No. 26 of April 17, 2002, as amended) regulates unsolicited marketing by email. Please see question 9.1.

(d) **Commercial Transactions**
The Act on Specified Commercial Transactions (Act No. 57 of June 4, 1976, as amended) regulates, among other forms of unsolicited marketing, unsolicited marketing by email. Please see question 9.1.

(e) **Utilisation of Numbers to Identify Individuals in Administrative Procedures**
The Japanese government adopted a social security and tax number system and in 2015, assigned specific numbers to entities and individuals pursuant to the Act on the Utilisation of Numbers to Identify Specific Individuals in Administrative Procedures (Act No. 27 of May 31, 2013, as amended; the "**My Number Act**"). The basic principle of this law is that using the assigned numbers will contribute to the efficient and prompt exchange of information by administrative organs. Under this law, the assigned numbers should be handled duly and safely in accordance with certain standards, which are different from those under the APPI and the laws described in items (ii) and (iii) of the laws listed in the first paragraph of the answer to question 1.1.

### 1.3 Is there any sector-specific legislation that impacts data protection?

The PPC was established on January 1, 2016, as the main agency to enforce and apply the APPI. While the PPC issues general guidelines on the implementation of the APPI (the "**PPC Guidelines**"), in some industries, other ministries also issue specific guidelines, such as (i) telecommunications guidelines issued by the MIC, (ii) broadcasting guidelines issued by the MIC, (iii) posting guidelines issued by the MIC, and (iv) genetic information guidelines issued by the Ministry of Economy, Trade and Industry. Further, the PPC and the Financial Services Agency have jointly issued certain financial affairs guidelines, while the PPC and the Ministry of Health, Labour and Welfare have jointly issued certain medical care guidelines.

### 1.4 What authority(ies) are responsible for data protection?

The PPC, as an independent regulatory body, is authorised to advise a Handling Operator or require it to prepare and submit a report on the handling of Personal Information to the extent necessary to implement the APPI (APPI, Articles 40 and 41). If a Handling Operator violates the APPI, the PPC may urge it to cease the violation and take other necessary measures to correct the violation (*Id.* Article 42, paragraph 1). If the PPC finds it necessary and certain requirements are met, it may order the Handling Operator to take the urged measures or to cease the violation and take other necessary measures to rectify the violation (*Id.* Article 42, paragraphs 2 and 3).

The PPC is also responsible for the supervision and enforcement of the My Number Act (My Number Act, Article 33).

Please also see question 1.1.

## 2 Definitions

### 2.1 Please provide the key definitions used in the relevant legislation:

- "**Personal Data**"
  The APPI provides for four definitions relevant to Personal Data:
  - "**Personal Information**" is information about living individuals which (a) can identify specific individuals, or (b) contains an "Individual Identification Code". Information which can identify specific individuals under clause (a) of the definition includes information which can be readily collated with other information to identify specific individuals.
  - The "**Individual Identification Code**" under clause (b) of the definition refers to any character, number, symbol or other code (i) into which a partial body feature of a specific individual has been converted by computers for use and which can identify such specific individual, or (ii) which is assigned to services or goods provided to an individual, or is stated or electromagnetically recorded on a card or other documents issued to an individual (such as a driver's licence number), to identify him/her as a specific user, purchaser, or recipient of the issued document (APPI, Article 2, paragraphs 1 and 2).
  - "**Personal Information Database**" means an assembly of information including the following: (i) an assembly of information systematically arranged in such a way that specific Personal Information can be retrieved by a computer; and (ii) an assembly of information designated by a Cabinet Order as being systematically arranged in such a way that specific Personal Information can be easily retrieved. However, any assembly of information the use of which is not likely to harm the interests of the individual principals, as further set out in the Cabinet Order of the APPI, is excluded from the definition (*Id.* Article 2, paragraph 4).
  - "**Personal Data**" means Personal Information constituting a Personal Information Database (*Id.* Article 2, paragraph 6).
- "**Retained Personal Data**" means Personal Data which a Handling Operator has the authority to disclose, correct, add, erase or delete, discontinue its utilisation, or discontinue its provision to a third party, excluding the following (*Id.* Article 2, paragraph 7):
  (i) any Personal Data, the existence or absence of which would harm the life, body or property of the relevant individual or a third party, encourage or solicit illegal or unjust acts, jeopardise the safety of Japan or harm the trust of or negotiations with other countries or international organisations, or impede crime investigations or public safety; or
  (ii) any Personal Data which will be erased from the Personal Information Database within six months after becoming part of the database. (Please note that the exclusion of this item (ii) from the definition of "Retained Personal Data" will cease to apply once the 2020 Amendment takes effect so that even Personal Data retained only for a period of six months or shorter will be subject to such obligations.)
  A Handling Operator is required to comply with obligations regarding Retained Personal Data under Articles 27 to 30 of the APPI. Please see question 5.1.

- "**Processing**"
  The APPI does not define "Processing". Although the APPI uses certain words such as handling (*toriatsukai*), obtaining (*shutoku*), utilisation (*riyou*), provisions (*teikyo*) to third parties and disclosure (*kaiji*), it does not define these words.
- "**Controller**"
  Please see the definition of "Processor" below.
- "**Processor**"
  The APPI does not use "Controller" or "Processor". However, a Handling Operator (*Kojin Joho Toriatsukai Jigyosha*) may be comparable to a Controller or a Processor in that it is subject to obligations to protect Personal Information. Please see question 1.1 for the definition of a Handling Operator. Foreign companies doing business in Japan will be regulated as Handling Operators if they fall within the definition.
- "**Data Subject**"
  The term "principal" would be comparable to a "Data Subject". Article 2, paragraph 8 of the APPI defines "principal" as a specific individual identified by Personal Information.
- "**Sensitive Personal Data**"
  "Sensitive Personal Data" is defined in the APPI as data referring to race, creed, social status, medical history, criminal record, whether one has been a victim of crime, and other Personal Information which needs careful handling so as not to cause social discrimination, prejudice or other disadvantages (APPI, Article 2, paragraph 3). The Cabinet Order for the APPI provides details of what constitutes Sensitive Personal Data, which include: physical or mental disabilities; results of medical examinations conducted by doctors or personnel who are engaged in medical services; records of medical treatment or medical advice provided based on the results of medical examinations or due to a disease, an injury or other changes in physical or mental conditions; and history related to criminal procedures such as arrest, investigation or detention.
- "**Data Breach**"
  "Data Breach" is not a term under the APPI; however, regarding Personal Data, the PPC's Notification No. 1 (2017) defines a breach of data security as a leakage of, loss of, or damage to data. Under the 2020 Amendment, Handling Operators will be required to notify the PPC of certain material breaches of data security. In the amendment to the Enforcement Ordinance of the APPI which will take effect in April 2022, material breaches include (i) leakage of, loss of, or damage to Personal Data including Sensitive Personal Data, (ii) leakage of, loss of, or damage to Personal Data which can be abused for economic gains, (iii) leakage of, loss of, or damage to Personal Data potentially caused by a malicious act, and (iv) leakage of, loss of, or damage to Personal Data where more than 1,000 principals are affected.
- "**Anonymously Processed Information**"
  "Anonymously Processed Information" is defined as information obtained by processing Personal Information such that ordinary people cannot (a) identify a specific principal using the processed information, or (b) restore any Personal Information from the processed information (APPI, Article 2.9). Anonymously Processed Information is not regulated as Personal Information since it does not identify any individual, but certain regulations apply, such as anonymising Personal Information in accordance with the PPC ordinance and guidelines and the prohibition against restoring Personal Information.

## 3 Territorial Scope

**3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?**

Most of the provisions applicable to Handling Operators under the APPI apply to business operators outside Japan if they receive Personal Information in connection with the provision of goods or services to individuals located in Japan (APPI, Article 75). Further, under the 2020 Amendment, all the provisions applicable to Handling Operators apply to those business operators outside Japan so that they may be subject to an obligation to report material data breaches to the PPC and to comply with orders issued by the PPC (please see question 16.4).

## 4 Key Principles

**4.1 What are the key principles that apply to the processing of personal data?**

- **Transparency**
  The APPI has no provision explicitly dealing with transparency. However, Handling Operators are required to either publicly announce or notify the principals of the purposes of utilisation of their Personal Information promptly after the collection of Personal Information (subject to certain exceptions) (APPI, Article 18).
  Further, the Basic Policy requires Handling Operators to establish and publicly disclose their privacy policy or privacy statement, as well as their use of service providers to handle collected Personal Information and the extent of the service.
- **Lawful basis for processing**
  Handling Operators are prohibited from acquiring Personal Information by deception or other wrongful means (*Id.* Article 17). They are also prohibited from acquiring Sensitive Personal Information without the consent of the principal except:
  (i) if required by laws and regulations;
  (ii) if necessary to protect the life, body, or property of a person and it is difficult to obtain the consent of the principal;
  (iii) if necessary to improve public health and promote the sound nurturing of the young and it is difficult to obtain the consent of the principal;
  (iv) if necessary for governmental bodies to perform their business and getting the consent of the principal will likely impede the proper performance of business; or
  (v) for Sensitive Personal Information that has been disclosed to the public by the principal, governmental bodies, or certain parties designated by the PPC (e.g., foreign governments and international organisations).
- **Purpose limitation**
  Handling Operators are required to specify the purposes of utilisation of Personal Information to the extent possible and not to use the Personal Information of any person, without obtaining the prior consent of that person, beyond the scope necessary to achieve the specified purpose of utilisation of Personal Information (*Id.* Articles 15 and 16). Further, Handling Operators are required to endeavour to keep Personal Information accurate and up to date within the scope necessary to achieve the purpose of utilisation of Personal Information (*Id.* Article 19).

- **Data minimisation**
  The APPI imposes no obligation to minimise the Personal Information which Handling Operators may obtain or use.
- **Proportionality**
  The APPI has no provision on proportionality.
- **Retention**
  Handling Operators are required to endeavour to delete Personal Information if its utilisation is no longer necessary (*Id.* Article 19). Further, there may be other restrictions under industry guidelines. For example, the MIC Guidelines provide that telecommunication business operators must fix the retention period for the purpose of utilisation of Personal Information, and erase Personal Information after the expiration of the retention period without delay (MIC Guidelines, Article 10).
- **Restriction on provision of Personal Data to a third party**
  A Handling Operator is prohibited from providing Personal Data to a third party without obtaining the prior consent of the principal, subject to certain exceptions (APPI, Article 23, paragraph 1), such as an "opt-out" arrangement under which the Handling Operator: (a) agrees to stop providing the Personal Data, which in this case does not include any Sensitive Personal Data, to the third party upon the demand of the principal; (b) notifies the principal of the provision to a third party or makes such notification readily accessible to the principal; and (c) submits a notification to the PPC stating (i) that the provision to third parties is included in the purpose of utilisation, (ii) the items to be provided to third parties, (iii) the mode of provision (e.g., by publishing a book or uploading to a website through the internet), (iv) the availability of opt-out for the principal who may request the Handling Operator to stop the provision, and (v) the mode of receiving the principal's request (e.g., telephone, email, or any written material) (*Id.* Article 23, paragraph 2). The 2020 Amendment enhances the items to be notified to the principals and the PPC and disallows "opt-out" arrangements in relation to the provision of any Personal Data collected in breach of the APPI and any Personal Data obtained using another "opt-out" arrangement.
- **Exceptions**
  The obligations imposed on Handling Operators will not apply to Handling Operators that fall under any of the following items and if all or part of the purpose of handling Personal Information is prescribed in the following applicable items (*Id.* Article 76):
  (i) broadcasting institutions, newspaper publishers, communication agencies and other forms of the press (including individuals engaged in news reporting as their business); for the purpose of news reporting;
  (ii) business operators in the business of literary work; for the purpose of literary work;
  (iii) colleges, universities, other institutions or organisations engaged in academic studies, or entities belonging to any of the foregoing entities; for the purpose of academic studies;
  (iv) religious organisations; for the purpose of religious activities (including activities incidental thereto); or
  (v) political organisations; for the purpose of political activities (including activities incidental thereto).

## 5 Individual Rights

### 5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**
  A Handling Operator is required to make accessible to the principal certain information (such as the name of the Handling Operator, the purpose of utilisation of Personal Information, and the procedures for notification of such information to the principal, correction of Personal Information or discontinuation of the utilisation of Personal Information) regarding Retained Personal Data (APPI, Article 27, paragraph 1). Further, the amendment to the Enforcement Ordinance of the APPI which will take effect in April 2022 provides that a Handling Operator will be required to make accessible to the principal the measures taken to secure Retained Personal Data except where the disclosure of such measures may endanger the security of the data itself.
  Further, if a person requests a Handling Operator to notify him/her of the purpose of utilisation of such Retained Personal Data which may lead to the identification of the person concerned, the Handling Operator must meet the request without delay, subject to certain exceptions (*Id.* Article 27, paragraph 2).
  The exceptions are cases where:
  (i) the purposes of utilisation are evident from the information made available to the person by the Handling Operators pursuant to Article 27, paragraph 1 of the APPI;
  (ii) publicly announcing or notifying the person of the purpose of utilisation is likely to harm the life, body, property, or other rights or interests of that person or a third party;
  (iii) publicly announcing or notifying the person of the purpose of utilisation is likely to harm the rights or legitimate interests of the Handling Operator; or
  (iv) it is necessary to cooperate with an administrative organ or a local government in implementing laws and regulations, and publicly announcing or notifying the person of the purpose of utilisation is likely to impede that implementation.
  In addition, the Handling Operator is required to disclose, without delay, and upon the request of an individual, that person's Retained Personal Data, subject to certain exceptions (*Id.* Article 28). The exceptions are cases where:
  (i) disclosure will likely harm the life, body, property, or other rights or interests of the person or a third party;
  (ii) disclosure will likely seriously impede the proper execution of the business of the Handling Operator; or
  (iii) disclosure will violate other laws and regulations.
  The Handling Operator may charge a fee for complying with a request to notify the purpose of utilisation pursuant to Article 27, or to disclose Retained Personal Data pursuant to Article 28.
- **Right to rectification of errors**
  The principal may request the Handling Operator to correct, add or delete Retained Personal Data if the Retained Personal Data are not correct. The Handling Operator must investigate without delay and, based on the

results of the investigation, correct, add or delete, as requested by the principal, the Retained Personal Data to the extent necessary to achieve the purposes of use (*Id.* Article 29).

- **Right to deletion/right to be forgotten**
  As above, the principal may request the Handling Operator to correct, add or delete Retained Personal Data if the Retained Personal Data are not correct. There is no explicit legal provision on the "right to be forgotten". Please see question 18.2 for the recent discussion regarding the "right to be forgotten".
- **Right to object to processing**
  The principal may request a Handling Operator (a) to discontinue the use of, or erase, the Retained Personal Data, and (b) to stop providing the Retained Personal Data to third parties if such use or disclosure is or was made, or the Retained Personal Data in question was obtained, in violation of the APPI. The Handling Operator must discontinue the use of, or the provision to third parties of, or erase, Retained Personal Data upon the request of the principal if the request has reasonable grounds (*Id.* Article 30). In addition, under the 2020 Amendment, the principal may request a Handling Operator (a) to discontinue the use of the Retained Personal Data and (b) to stop providing the Retained Personal Data to third parties if the Handling Operator ceases to have any reason to use the Retained Personal Data, a material data breach has occurred, or the right or legitimate interest of the principal may be harmed for any other reasons.
  However, these obligations will not apply if it will be too costly or difficult to discontinue the use of, or to erase, the Retained Personal Data and the Handling Operator takes necessary alternative measures to protect the rights and interests of the principal.
- **Right to restrict processing**
  There is no "right to restrict processing" which differs from the rights stipulated above in "Right to object to processing".
- **Right to data portability**
  While legal problems regarding data portability have been the subject of recent intensive discussions, no specific laws or regulations regarding data portability exist to date.
- **Right to withdraw consent**
  There is no explicit stipulation regarding the right to withdraw consent under the APPI.
- **Right to object to marketing**
  There are no provisions explicitly setting forth objections to marketing. Any objection to marketing would be dealt with as an objection to processing.
- **Right to complain to the relevant data protection authority(ies)**
  The individuals may complain to the PPC and the PPC will conduct necessary mediation regarding a lodged complaint (*Id.* Article 61(ii)).
- **Complaint to Authorised Entities for Protection of Personal Information (*Nintei Kojin Jyouhou Hogo Dantai*)**
  Authorised Entities for the Protection of Personal Information (*Nintei Kojin Jyouhou Hogo Dantai*) are entities authorised by the PPC to handle complaints from individuals on the handling of Personal Information by their respective member Handling Operators ("Member Handling Operators"). As of March 10, 2021, 41 entities have obtained such authorisation.
  When an Authorised Entity for the Protection of Personal Information is requested by an individual to resolve a complaint about the handling of Personal Information by a Member Handling Operator, it must promptly notify the Member Handling Operator of the complaint and give necessary advice, investigate the circumstances pertaining to the complaint and request the Member Handling Operator to resolve the complaint promptly. It may, if necessary, request the Member Handling Operator to explain in writing or orally, or request it to submit relevant materials. The Member Handling Operator may not reject such request without a justifiable ground (*Id.* Article 52).

## 6 Registration Formalities and Prior Approval

**6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?**

The APPI imposes no requirement on a Handling Operator to register or notify the PPC to process Personal Information. However, if the Handling Operator provides Personal Information to third parties without obtaining the prior consent of the principals under an "opt-out" arrangement, it is required to notify the PPC (please see question 4.1).

The PPC is also authorised to enter offices or other places, to make inquiries and investigate, and to require a Handling Operator to report or submit materials regarding the handling of Personal Information or Anonymously Processed Information, to the extent necessary to implement the APPI (*Id.* Articles 40 and 41). Please see question 1.4.

**6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?**

Please see question 6.1.

**6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?**

Please see question 6.1.

**6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?**

Please see question 6.1.

**6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?**

Please see question 6.1.

**6.6 What are the sanctions for failure to register/notify where required?**

Please see question 6.1.

**6.7 What is the fee per registration/notification (if applicable)?**

Please see question 6.1.

**6.8 How frequently must registrations/notifications be renewed (if applicable)?**

Please see question 6.1.

**6.9 Is any prior approval required from the data protection regulator?**

Please see question 6.1.

**6.10 Can the registration/notification be completed online?**

Please see question 6.1.

**6.11 Is there a publicly available list of completed registrations/notifications?**

Please see question 6.1.

**6.12 How long does a typical registration/notification process take?**

Please see question 6.1.

## 7 Appointment of a Data Protection Officer

**7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.**

The APPI has no provision mandating the appointment of a Privacy or Data Protection Officer. However, the Handling Operator is required to take necessary and proper measures for the prevention of leakage, loss, or damage, and for other security control, of Personal Data (APPI, Article 20). Under the PPC Guidelines, those measures should include the following:

(i) organisational security measures, such as establishing rules for handling Personal Data, and specifying the person responsible for supervising the handling of Personal Data;
(ii) human resource security measures, including the education of employees;
(iii) physical security measures, including controlling the area where Personal Data is handled, such as servers and offices; and
(iv) technical security measures, including controlling access to Personal Data.

The PPC Guidelines indicate that appointing a person to be in charge of the handling of Personal Data is an example of a proper and necessary measure.

**7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?**

Although a Handling Operator is expected to adopt the measures described in the PPC Guidelines, the failure to adopt such measures is not a direct breach of the APPI.

**7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?**

There is no special protection.

**7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?**

Please see question 7.1.

**7.5 Please describe any specific qualifications for the Data Protection Officer required by law.**

Please see question 7.1.

**7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?**

Please see question 7.1.

**7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?**

There is no requirement for the appointment of a Data Protection Officer to be registered or notified.

**7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?**

There is no requirement for a Data Protection Officer to be named in a public notice.

## 8 Appointment of Processors

**8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?**

There is no concept of "processor" under the APPI (please see question 2.1). However, there is a concept of "entrustment" of the handling of Personal Data in which entering into an agreement is recommended.

Under Article 23, paragraph 5(i) of the APPI, if the Handling Operator entrusts all or part of the handling of the Personal Data it acquires to an individual or another entity, that individual or entity will not be considered a "third party" under Article 23, paragraph 1.

For example, if the Handling Operator uses third-party vendors for the services, and it shares Personal Data with those third-party vendors for them to use on the Handling Operator's behalf, and not for their own use, such transfer will be deemed

an "entrustment" and the restrictions on the provision of Personal Data to a third party will not apply.

When the Handling Operator "entrusts" Personal Information, it must exercise the necessary and appropriate supervision over the entrusted person to ensure security control over the entrusted Personal Data. The Handling Operator must ensure that the entrusted person (e.g., the third-party service provider) has taken the same appropriate measures that the Handling Operator is required to take. The PPC Guidelines provide that "necessary and appropriate supervision" includes appropriately selecting the service provider, concluding the necessary contracts so that the security control measures based on Article 20 of the APPI are observed by the service provider, and knowing the status of the handling of the Personal Data that was entrusted to the service provider.

**8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?**

PPC Guidelines provide that it is desirable to include the agreed security control measures and a provision that allows the Handling Operator to reasonably understand the status of the handling of Personal Data by the service provider.

## 9 Marketing

**9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).**

Unsolicited marketing by email is regulated principally by the Act on the Regulation of the Transmission of Specified Electronic Mail (Act No. 26 of April 17, 2002, as amended; the "**Anti-Spam Act**"). Pursuant to the Anti-Spam Act, marketing emails can be sent only to recipients who (i) "opted in" to receive them, (ii) provided the sender with their email address in writing (for instance, by providing a business card), (iii) have a business relationship with the sender, or (iv) make their email address available on the internet for business purposes. In addition, the Anti-Spam Act requires the senders to allow the recipients to "opt out". The Act on Specified Commercial Transactions also adopts the opt-in system for unsolicited marketing.

**9.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?**

The Anti-Spam Act applies not only to business-to-consumer marketing but also to business-to-business marketing.

**9.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).**

Unsolicited telephone marketing regarding certain items such as financial instruments (e.g., derivatives) is restricted under different regulations. There is no national opt-out register system.

**9.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?**

The Anti-Spam Act will apply to any entity, whether or not it has a presence in Japan, even if its marketing emails are sent from outside Japan, as long as the receiver is in Japan.

**9.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?**

The MIC and the Consumer Affairs Agency are the authorities in charge of enforcement of the Anti-Spam Act. There have been several enforcement cases initiated by those authorities, including a recent enforcement in March 2018.

**9.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?**

Purchasing a marketing list is not, in itself, illegal. However, the seller must obtain the consent of the principals, unless an exemption from the consent requirement applies. In addition, the seller must keep a record of certain information related to the provision of Personal Data for three years, and the purchaser must be informed of the name and address of the seller, the name of the seller's representative and how the seller obtained the list, and must keep a record thereof for three years (APPI, Articles 25 and 26).

**9.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?**

The maximum penalties under the Anti-Spam Act are one year of imprisonment or a fine of 1,000,000 yen for an individual, and a fine of 30,000,000 yen for the legal entity which employed that individual.

The maximum penalty for breaching the APPI is currently either imprisonment of up to one year or a fine of up to 1,000,000 yen for individuals and 100,000,000 yen for legal entities (APPI, Articles 83 and 87).

## 10 Cookies

**10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).**

The use of cookies or other similar technology is not directly regulated under the current APPI unless such use enables the identification of an individual by combining the data obtained with other data; however, if Personal Data is collected through such technology, such Personal Data is subject to the APPI.

However, the 2020 Amendment will regulate "Related Personal Information" or information which is related to a living individual but cannot, by that information alone, identify the individual. When the 2020 Amendment takes effect, cookies will be deemed Related Personal Information and cannot be provided to a third party if that third party may be able to use the cookies to identify an individual, except where the business operator has confirmed that the principal has given consent.

**10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?**

The 2020 Amendment does not distinguish between different types of cookies as long as a principal can be identified by combining cookies and other data.

**10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?**

The 2020 Amendment has not yet taken effect.

**10.4 What are the maximum penalties for breaches of applicable cookie restrictions?**

Currently, there are no penalties. The 2020 Amendment, however, will impose an administrative fine of up to 100,000 yen on a provider of Related Personal Information who falsely declares that it has obtained the required consent.

## 11 Restrictions on International Data Transfers

**11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.**

The prior consent of the principals is required to transfer their Personal Information to a third party located in a foreign country (APPI, Article 24). However, the principals' prior consent to overseas data transfers of their Personal Information is not necessary if (i) the foreign country is specified in the PPC Ordinance as having a data protection regime with a level of protection equivalent to that of Japan, or (ii) the third-party recipient has a system of data protection which meets the standards to be prescribed by the PPC Ordinance.

As of January 23, 2019, the PPC has specified the EU and the UK as having a data protection regime with a level of protection equivalent to that of Japan by the PPC Ordinances (item (1) above). As of the same date, the European Commission also adopted the adequacy decision on Japan in accordance with Article 45 of the GDPR.

The PPC issued the Supplementary Rules for Personal Data, which have been transferred from the EU and the UK by the adequacy decision. By the Supplementary Rules, the Handling Operators are subject to stricter regulations with regard to Personal Data, which have been transferred from the EU by the adequacy decision.

The PPC Ordinance also provides that with respect to item (ii), the third-party foreign recipient must either (a) provide assurance by appropriate and reasonable methodologies that it will treat the transferred Personal Information pursuant to the spirit of the requirements for the handling of Personal Information under the APPI, or (b) have been certified under a PPC-recognised international arrangement regarding its system of handling Personal Information (to date, the only PPC-recognised international arrangement is the APEC Cross-Border Privacy Rules System).

**11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).**

Please see question 11.1.

**11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.**

Please see question 11.1.

**11.4 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?**

The PPC has not issued any guidance following the decision of the Court of Justice of the EU in *Schrems II*, probably because the adequacy decision on Japan would not be affected by the court decision.

**11.5 What guidance (if any) has/have the data protection authority(ies) issued in relation to the European Commission's revised Standard Contractual Clauses?**

The PPC has not issued any guidance regarding the revised Standard Contractual Clauses.

## 12 Whistle-blower Hotlines

**12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?**

The Whistle-Blower Protection Act (*Kouekі Tsuhosha Hogo Hou*) prohibits employers from dismissing whistle-blowers. The current Act itself does not have requirements for companies to have a whistle-blower hotline or system, but the Consumer Affairs Agency has published guidelines for private entities to establish and operate whistle-blower hotlines. The guidelines also specify several measures which companies must implement to protect the Personal Information of whistle-blowers, such as limiting the persons who can access documents regarding the whistle-blowing. Under the amendment to this Act, which will take effect by June 2022, business operators employing more than 300 employees will be required to, while business operators employing 300 or fewer employees will be required to endeavour to, appoint a responsible person who will receive reports, investigate and take remedial measures, and take other measures to protect whistle-blowers.

**12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?**

Anonymous reporting is generally permitted.

## 13 CCTV

**13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?**

There are no registration/notification requirements for the use of CCTV under the APPI. However, according to the Q&A regarding the PPC Guidelines published by the PPC, it is desirable to take measures so that the individual in question may recognise that his/her Personal Information is being obtained, through visible notices stating that CCTV is in operation. Further, it is desirable to display contact information, a website URL or a QR code in a notice located near CCTV, so that the individual may confirm the relevant information regarding the CCTV.

**13.2 Are there limits on the purposes for which CCTV data may be used?**

There are no special restrictions for CCTV data which differ from restrictions on other Personal Data under the APPI.

## 14 Employee Monitoring

**14.1 What types of employee monitoring are permitted (if any), and in what circumstances?**

The employer has the right to monitor workplace communications in relation to work. However, a privacy issue may arise regarding private communications in the workplace. Thus, it is recommended that employers establish internal rules prohibiting the use of company PCs and email addresses for private use, and disclosing the possibility of monitoring those devices and data.

**14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.**

Please see question 14.3.

**14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?**

There are no statutory and special requirements for notification to or consultation with trade unions/employee representatives regarding employee monitoring. However, if an employer sets up internal rules on employee monitoring, these rules will be considered company work rules and would require prior notification to or consultation with the majority union or employee representative.

## 15 Data Security and Data Breach

**15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?**

A Handling Operator is obligated to take necessary and proper measures to prevent leakage, loss, or damage, and for other security control, of Personal Data (APPI, Article 20). Further, the Handling Operator is required to exercise necessary and appropriate supervision over its employees and service providers to ensure the security control of Personal Data (*Id.* Articles 21 and 22). There is no concept of controllers or processors under the APPI (please see question 2.1).

**15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

Currently, there is no reporting requirement under the APPI, and the PPC's Notification only provides that a Handling Operator must endeavour to report a breach to the government through the PPC, an Accredited Personal Information Protection Organisation, or any other supervising authority or organisation. However, reporting is not required in the following cases:

(i) the Handling Operator has determined that a Personal Data leakage is not substantial; or

(ii) there have been only minor wrong transmissions of email or fax or erroneous dispatch of a package.

Under the financial affairs guidelines (please see question 1.3), a Handling Operator in the financial sector must report any leakage of Personal Information to the Financial Services Agency immediately.

The 2020 Amendment will introduce an obligation to report material data breaches (please see question 2.1) to Personal Data to the PPC.

**15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

The PPC's Notification provides that it is preferable for a Handling Operator to notify the principal who may be affected by the data breach in order to prevent further damage, and to publicly announce the fact of the data breach and its recurrence prevention measure in order to prevent further damage and similar data breaches in other companies.

The 2020 Amendment will require a Handling Operator to report material data breaches relating to Personal Data to the affected data subjects unless it is difficult to make that report and an alternative measure is taken. A Handling Operator will be required to report a material data breach to the PPC within 30 days (or 60 days with regard to a data breach potentially caused by a malicious act) after the data breach becomes known to the Handling Operator.

**15.4 What are the maximum penalties for data security breaches?**

If a Handling Operator provides or misuses a Personal Information Database for the purpose of unlawful gains, it may be subject to imprisonment of up to one year, or a fine of up to 1,000,000 yen (*Id.* Article 83). If the breach is committed by a person who is employed by an entity, such entity will be subject to a fine of up to 100,000,000 yen (*Id.* Article 87).

## 16 Enforcement and Sanctions

**16.1 Describe the enforcement powers of the data protection authority(ies).**

(a) **Investigative Powers**: The PPC may require a Handling Operator to report or submit materials regarding its handling of Personal Information, enter offices or other places to conduct an investigation, make inquiries and check records or other documents (*Id.* Article 40), and require an Authorised Entity for the Protection of Personal Information to report regarding its activities (*Id.* Article 56).

(b) **Corrective Powers**: The PPC may render guidance or advice to a Handling Operator (*Id.* Article 41), recommend a Handling Operator to cease the violation, take necessary measures to correct the violation and other necessary measures (*Id.* Article 42) and order an Authorised Entity for the Protection of Personal Information to take necessary measures (*Id.* Article 57).

(c) **Authorisation and Advisory Powers**: The PPC does not have a general authorisation or advisory power, but has the authority to grant authorisation to applicant entities to become Authorised Entities for the Protection of Personal Information.

(d) **Imposition of administrative fines for infringements of specified GDPR provisions**: The PPC will enforce their investigating or corrective powers under the APPI, but does not have the authority to enforce GDPR provisions.

(e) **Non-compliance with a data protection authority**: If an order issued by the PPC is breached, an individual may be subject to imprisonment of up to one year, or a fine of up to 1,000,000 yen (*Id.* Article 83), and the legal entity employing the individual will also be subject to a fine of up to 100,000,000 yen (*Id.* Article 87).

**16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?**

In relation to the PPC's powers stated in question 16.1 above, the PPC would have the power to issue an order to ban a particular processing activity without the need for a court order.

**16.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.**

The PPC has rendered guidance and recommendations, neither of which can impose any penalty for failure to comply, but has not rendered any order for which a penalty may be imposed for non-compliance with the order. In general, the PPC renders guidance in the case of a relatively less important violation, and a recommendation in the case of a more important violation. In a case in December 2019, the PPC rendered guidance to 35 data recipients and a recommendation to a data provider.

**16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?**

The enforcement powers of the PPC against foreign companies were introduced on May 30, 2017. Currently, among the enforcement measures stated in question 16.1, the PPC's enforcement power is limited to (i) rendering guidance or advice to a Handling Operator (Article 41), and (ii) recommending a Handling Operator to cease the violation and take other necessary measures to correct the violation (Article 42.1). The 2020 Amendment grants to the PPC the authority to issue an order to take remedial measures to Handling Operators which receive Personal Information in connection with the provision of goods or services to individuals located in Japan (Article 42.2).

## 17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

**17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?**

Under the APPI, the general rule is that the Handling Operator cannot provide Personal Data to any "third party" without obtaining the prior consent of the principal, except in specified cases (Article 23.1). These specified cases are cases where the provision of Personal Data is:

(i) required by laws and regulations;

(ii) necessary to protect the life, body, or property of a person and it is difficult to obtain the consent of the principal;

(iii) necessary to improve public health and promote the sound nurturing of the young and it is difficult to obtain the consent of the principal; and/or

(iv) necessary for governmental bodies to perform their business and getting the consent of the principal will likely impede the proper performance of business.

It is understood that "governmental bodies" referenced in (iv) above would be bodies of the Japanese government and not of other countries, and "laws" referenced in (i) above would not include foreign laws. If the Handling Operator were compelled to disclose Personal Information of Japanese individuals in accordance with a foreign law or by an action of a foreign governmental institution, the Handling Operator may be able to disclose the personal data in accordance with (ii) above; however, to avoid any risk in this regard, it is practical to obtain the prior consent of the data owners before transferring data in response to requests from foreign law enforcement agencies.

**17.2 What guidance has/have the data protection authority(ies) issued?**

There is no specific guidance by PPC regarding the response to foreign e-discovery requests or requests for disclosure from foreign law enforcement agencies.

## 18 Trends and Developments

### 18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

As per questions 1.1 and 1.4, the PPC, as an independent regulatory body, has the authority to enforce the PPC as of May 30, 2017. The enforcement cases brought by the PPC regarding the APPI in FY 2019 (April 2019 to March 2020) were: 357 cases where the PPC required Handling Operators to report or submit materials regarding their handling of Personal Information; and 131 cases where the PPC rendered guidance or advice.

### 18.2 What "hot topics" are currently a focus for the data protection regulator?

As discussed above, the 2020 Amendment, which will take full effect by June 2022, will strengthen regulations in various areas such as cookies, penalties, reporting obligations, and extraterritorial enforcement. On the other hand, the 2020 Amendment will provide certain exemptions from APPI obligations so that a Handling Operator may use Personal Information for data analysis or other purposes if it removes certain descriptions (such as names) from the Personal Information (referred to as "**Pseudonymised Information**") so that any individual cannot be identified without combining the Pseudonymised Information with other data which the Handling Operator is allowed to retain.

**Hiromi Hayashi** is a partner at Mori Hamada & Matsumoto, which she joined in 2001. She specialises in communications law and regulation and authored the Japanese section of *Telecommunication in Asia* in 2005. Her other areas of practice are international and domestic transactions, takeover bids and corporate restructuring. Hiromi was admitted to the Bar in 2001 in Japan and in 2007 in New York. She worked at Mizuho Corporate Bank from 1989 to 1994 and at Davis Polk & Wardwell in New York from 2006 to 2007.

**Mori Hamada & Matsumoto**
Marunouchi Park Building, 2-6-1
Marunouchi Chiyoda-ku
Tokyo 100-8222
Japan

Tel: +81 3 5220 1811
Email: hiromi.hayashi@mhm-global.com
URL: www.mhmjapan.com

**Masaki Yukawa** is a counsel at Mori Hamada & Matsumoto, which he joined in 2009. He advises on Japanese data protection issues for technology companies, e-commerce companies and financial institutions. He was admitted to the Bar in 2009 in Japan and in 2016 in California. He was with the Bank of Japan from 2003 to 2008 and the Financial Services Agency from 2014 to 2015.

**Mori Hamada & Matsumoto**
Marunouchi Park Building, 2-6-1
Marunouchi Chiyoda-ku
Tokyo 100-8222
Japan

Tel: +81 3 5220 1811
Email: masaki.yukawa@mhm-global.com
URL: www.mhmjapan.com

Mori Hamada & Matsumoto is a full-service international law firm based in Tokyo with offices in Bangkok, Beijing, Shanghai, Singapore, Yangon and Ho Chi Minh. The firm has over 600 attorneys and a support staff of approximately 550 people, including legal assistants, translators and secretaries. The firm is one of the largest law firms in Japan and is particularly well known in the areas of mergers and acquisitions, finance, litigation, insolvency, telecommunications, broadcasting and intellectual property, as well as domestic litigation, bankruptcy, restructuring and multi-jurisdictional litigation and arbitration. The firm regularly advises on some of the largest and most prominent cross-border transactions, representing both Japanese and foreign clients. In particular, the firm has extensive practice in, exposure to and expertise on telecommunications, broadcasting, internet, information technology and related areas, and provides legal advice and other legal services regarding the corporate, regulatory, financing and transactional requirements of clients in these areas.

**www.mhmjapan.com**

MORI HAMADA & MATSUMOTO

# Korea


Iris Hyejin Hwang


Hye In Lee

D'LIGHT Law Group



## 1 Relevant Legislation and Competent Authorities

### 1.1 What is the principal data protection legislation?

The Personal Information Protection Act ("**PIPA**") regulates data protection, from the establishment of national policies on Personal Information protection to detailed procedures and methods of Personal Information Processing and protection.

### 1.2 Is there any other general legislation that impacts data protection?

Apart from PIPA, there is no other general legislation that governs data protection in particular.

### 1.3 Is there any sector-specific legislation that impacts data protection?

The Credit Information Use and Protection Act ("**Credit Information Act**") regulates "Credit Information", meaning information relating to a person's credit that can identify such person, or information that can determine the transaction details, creditworthiness, or credit transaction capacity of such person.

The Act on the Protection, Use, Etc. of Location Information ("**Location Information Act**") regulates the location information of a person.

### 1.4 What authority(ies) are responsible for data protection?

The Personal Information Protection Commission ("**PIPC**") under the Prime Minister's office is the major authority responsible for data protection. PIPC oversees the protection of Personal Information (defined below) by: i) improving laws relating to Personal Information protection; ii) establishing or executing policies, systems, or plans relating to Personal Information protection; iii) investigating infringements of the rights of Data Subjects (defined below), and any ensuing dispositions; and iv) managing complaints or remedial procedures about Personal Information Processing and mediation of disputes over Personal Information. PIPC has jurisdiction over the interpretation and operation of law related to Personal Information protection.

PIPC assigned the Korea Internet & Security Agency ("**KISA**") as the exclusive authority to receive Personal Information divulgence reports. PIPC also entrusted KISA with rights and obligations including education of public, training of specialists, investigation of divergence cases, and more.

The Financial Services Commission ("**FSC**") oversees credit information businesses and their compliance with the Credit Information Act, with the power to order any violating company to take corrective measures.

The Korea Communications Commission ("**KCC**") is in charge of businesses handling personal location information and their compliance with the Location Information Act. In case of non-compliance, KCC may revoke the permission granted to a location information provider or a location-based service provider through a cease-and-desist order on operations, from a certain duration up to a permanent basis.

## 2 Definitions

### 2.1 Please provide the key definitions used in the relevant legislation:

- "**Personal Data**"
  Any of the following information relating to a living individual:
  (a) information that identifies an individual by his or her full name, resident registration number, image, etc.;
  (b) information which, by itself, does not identify an individual, but may be easily combined with other information to identify an individual. The ease of combination is determined by reasonably considering the time, cost, technology, etc. used to identify the individual and the likelihood that the other information can be procured; or
  (c) information under items (a) or (b) that is pseudonymised, and thereby becomes incapable of identifying an individual without the use or combination of information that restores the information to its original state ("**Pseudonymized Information**").
- "**Processing**"
  The collection, generation, connecting, interlocking, recording, storage, retention, value-added processing, editing, searching, output, correction, recovery, use, provision, disclosure, and destruction of Personal Information, and other similar activities.
- "**Controller**"
  Defined as "Personal Information Controller" in PIPA, means a public institution, legal person, organisation, individual, etc. that processes personal information directly or indirectly to operate the personal information files as part of its activities.

- "**Processor**"
  Defined as "Outsourcee" for an entity that processes Personal Information under an outsourcing contract with the Controller.
- "**Data Subject**"
  An individual who is identifiable through the information processed and is the subject of that information.
- "**Sensitive Personal Data**"
  Defined as "sensitive information" in PIPA, means any information prescribed by Presidential Decree, including ideology, belief, admission to or withdrawal from a trade union or political party, political opinions, health, sex life, and other personal information that is likely to markedly threaten the privacy of any Data Subject. The Presidential Decree includes i) DNA information, ii) criminal records, iii) physical, physiological or behavioural character information, generated by certain technics to identify a specific individual from another, and iv) race or ethnicity information.
- "**Data Breach**"
  Defined as "Divulgence, Etc." in PIPA, refers to instances when Personal Information is lost, stolen, or divulged. However, the term Divulgence, Etc. is used only to indicate the occasions when an ICSP is obliged to notify users or report the authority. In other cases, PIPA describes a data breach as Personal Information that is lost, stolen, divulged, forged, altered, or damaged.
- "**Pseudonymisation**"
  A procedure to process Personal Information so that the information cannot identify a particular individual without additional information, by deleting in part, or replacing in whole or in part, such information.
- "**Personally Identifiable Information**"
  Information that is assigned in accordance with the statute to uniquely identify an individual. There are four types of Personally Identifiable Information, which are the resident registration number, driver's licence number, passport number, and alien registration number.
- "**Information and Communications Service Provider**" **or** ("**ICSP**")
  Any person who: i) allows other parties to communicate with each other through the use of machinery, lines, or other facilities/equipment necessary to transmit or receive codes, speech, sound, or images by wire, wireless connection, light, or other electronic methods; ii) provides the facilities to communicate with others; or iii) conducts business to provide information or allow the provision of information using those facilities.
- "**Outsource**" and "**Supply**"
  Both refer to the Controller's provision of Personal Information to a third party. Outsourcing occurs when a Controller subcontracts part of its own work and the subcontractor needs to Process Personal Information. On the other hand, Supply occurs when a Controller transfers Personal Information to a third party for use and benefit of such third party.

## 3 Territorial Scope

### 3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

PIPA applies to entities established outside Korea. Specifically, any large-sized ICSP (person or corporation) or any large-sized third party who receives Personal Information from ICSP ("**ICSP-related Party**") under the Data Subject's consent or under law does not have an address or office in Korea must designate a local agent to act on its behalf. An ICSP or a third party will be considered large when 1) its global sales for the preceding year equals to or exceeds KRW 1 trillion, 2) its sales in Korea from information and telecommunications services for the preceding year equals to or exceeds KRW 10 billion, 3) it deals with equal to or more than 1 million users' Personal Information (average number of users per day over the three months immediately before the end of the preceding year), or 4) it has been required by the KCC to submit materials or documents because it caused or is likely to have caused a Personal Information breach in violation of PIPA.

PIPA does not explicitly state its extraterritorial reach in other provisions, but it is typically understood that other provisions are applicable to foreign persons or corporations also.

## 4 Key Principles

### 4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  Controllers must make their privacy policy and other matters related to Personal Information Processing public, explicitly state the purposes for which Personal Information is Processed and guarantee the Data Subject's rights such as access right.
- **Lawful basis for processing**
  Controllers must collect any Personal Information lawfully and fairly, and endeavour to obtain the trust of Data Subjects by observing and performing the duties and responsibilities required in PIPA and other related statutes.
- **Purpose limitation**
  Controllers must ensure that Personal Information is Processed in an appropriate manner within the scope of the stated purposes.
- **Data minimisation**
  Controllers must collect Personal Information to the minimum extent necessary for the stated purposes.
- **Proportionality**
  Please see above.
- **Retention**
  The Controller must manage Personal Information safely considering the possibility and severity of infringement on the Data Subject's rights in accordance with the processing methods, Personal Information types and such. The Controller must destroy Personal Information without delay when the Personal Information becomes unnecessary including but not limited to the expiry of the retention period or the fulfilment of the Processing purpose, unless required otherwise by another statute.

- *Other key principles*
  If the stated purpose can be fulfilled by processing anonymised or pseudonymised Personal Information, the Controller shall endeavour to process Personal Information through anonymisation where possible, or through pseudonymisation otherwise.

## 5 Individual Rights

### 5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**
  The Data Subject may request access to his/her Personal Information to the Controller. The Controller must let the Data Subject access the Personal Information within 10 days of its receipt of a request, absent reasons stated under PIPA to limit such access rights such as possibility to cause damage to the life or body of a third party, infringement of property, delay in government authority's work and others.
- **Right to rectification of errors**
  The Data Subject may send a request to the Controller for the correction of his/her Personal Information. The Controller must correct the Personal Information and notify the Data Subject of the change within 10 days of its receipt of the request.
- **Right to deletion/right to be forgotten**
  Unless the collection of certain Personal Information is mandatorily required by statute, the Data Subject may request that the Controller delete certain Personal Information. The Controller must delete the requested Personal Information and notify the Data Subject within 10 days of its receipt of the request.
- **Right to object to processing**
  The Data Subject may request the relevant Controller to suspend the processing of his/her Personal Information. Unless there are exceptions under PIPA, the Controller must suspend the processing of such Personal Information and notify the Data Subject of the status within 10 days of its receipt of the request.
- **Right to restrict processing**
  Nothing under Korean law grants Data Subjects with the right to restrict processing.
- **Right to data portability**
  PIPA does not grant the Data Subject with the right to data portability. However, under the Credit Information Act, a Data Subject of credit information may request his/her credit information to be transmitted to itself or to a certain third party regulated by the Credit Information Act.
- **Right to withdraw consent**
  A Data Subject may withdraw his/her consent provided to an ICSP or ICSP-related party. Once a Data Subject withdraws his/her consent, ICSP or the ICSP-related party must immediately take necessary measures, such as destroying the Personal Information in a way so that it cannot be recovered. The Data Subject's withdrawal rights to Controllers other than the ICSP or ICSP-related party is not found in PIPA.
  In the Credit Information Act, a Data Subject may withdraw consent to the transmission of his/her personal credit information from a credit information provider to another.
- **Right to object to marketing**
  When obtaining consent to process Personal Information for the purpose of marketing, the Controller must clearly notify such purpose to the Data Subjects, and the Controller's provision of its goods or services shall not be impacted by the Data Subject's consent for marketing.
- **Right to complain to the relevant data protection authority(ies)**
  Anyone who suffers an infringement of rights or interests over one's Personal Information during Personal Information Processing by a Controller may report such infringement to government authorities, and KISA is the designated special agency for receiving and processing such reports.
- **Notification of the Use History of Personal Information**
  The ICSP or the ICSP-related party, in meeting the requirements prescribed by the PIPA Presidential Decree, must notify users of the use history of their Personal Information on a regular basis. This does not apply where the collected information not including contact information enables notification to users.

## 6 Registration Formalities and Prior Approval

### 6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

In general, businesses have no legal obligation to register with nor notify the data protection authorities in respect of processing activities. However, businesses who collect a certain type of information may need to register with or notify a relevant protection authority.

In particular, a location-based service business that provides services based on personal location information needs to be reported to the KCC, while location information business that collects and provides personal location information to location-based service providers must obtain a business permit from the KCC. It should also be noted that if only non-personal or object location information is to be handled in relation to the business, location-based service businesses have no obligation to report any objective location information to the KCC.

### 6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

For a location information business permit, the KCC will review the feasibility of the business plan, technical and managerial measures for personal location information protection, the size of location information facilities, financial and technical capabilities and such. Accordingly, applicants are required to submit specific information for certain items, such as 1) the layout of location information processing systems including parts, processing technical, collection routes and collection servers, and the function of each system parts, access technical and communication methods between parts etc., 2) process to obtain or withdraw consent for location information collection,

and 3) records for location information process including data fields and automatic recording systems, and more.

When reporting to the KCC, a business plan, including the status of the service provider and the details of its business, the details and location of the main facilities for its business, and the measures for information protection is required.

**6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?**

Each registration/notification is made per legal entity.

**6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?**

Any legal entity, foreign or local, intending to engage in the businesses outlined in question 6.1 must either apply for permission or file a report as set out in question 6.2.

**6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?**

Please refer to the answer to question 6.2.

**6.6 What are the sanctions for failure to register/notify where required?**

An entity in violation of an aforementioned business permit, business report or notification of change can be either punished by imprisonment or a fine. The maximum limit of punishment will be five years of imprisonment with labour and/or 50 million KRW in the case of a business permit, three years of imprisonment with labour and/or 30 million KRW in the case of a report and one year of imprisonment with labour and/or 20 million KRW in the case of notification.

**6.7 What is the fee per registration/notification (if applicable)?**

There is no fee to be paid for the purpose of business permit or report.

**6.8 How frequently must registrations/notifications be renewed (if applicable)?**

A renewal procedure is not required for such registration or report. However, when there is any change in the legal entity's trade name, principal place of business or location information system, the legal entity must report the change to the KCC.

**6.9 Is any prior approval required from the data protection regulator?**

Please refer to the answer to question 6.2.

**6.10 Can the registration/notification be completed online?**

Yes, registration/notification may be completed at https://www.emsit.go.kr/ (only available in Korean).

**6.11 Is there a publicly available list of completed registrations/notifications?**

Yes, please see https://kcc.go.kr/user.do?boardId=1030&page=A02060400&dc=K02060400 (only available in Korean). However, KCC does not update the list frequently.

**6.12 How long does a typical registration/notification process take?**

It normally takes about two months for a business permit, and two weeks for confirmation on report.

## 7 Appointment of a Data Protection Officer

**7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.**

Anyone who processes Personal Information directly or indirectly to operate one or more Personal Information Files as part of its activities must appoint a Data Protection Officer ("**DPO**").

**7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?**

Anyone required to appoint a DPO that fails to do so could be administratively fined up to 10 million KRW.

**7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?**

The DPO may not be subject to disadvantages without justifiable grounds by its employer for performing the functions of the role required by PIPA.

**7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?**

The DPO of a legal entity must be the owner of the business, its representative, or its executive officer. In the case that a legal entity lacks an executive officer, the head of a department in charge of the affairs related to Personal Information Processing may become the DPO. In theory, if a person holds a position in two different entities that meet the requirement, he/she could become the DPO of both legal entities.

**7.5 Please describe any specific qualifications for the Data Protection Officer required by law.**

Please refer to the answer to question 7.4.

**7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?**

The DPO must: i) establish and implement a Personal Information protection plan; ii) conduct a regular survey of the status and practices of Personal Information Processing, and improve shortcomings; iii) handle complaints and remedial compensation in relation to Personal Information Processing; iv) build the internal control system to prevent the leak, abuse, and misuse of Personal Information; v) prepare and implement an education programme about Personal Information protection; vi) protect, control, and manage the Personal Information Files; vii) establish, modify, and implement a privacy policy pursuant to PIPA; viii) manage materials related to the protection of Personal Information; and ix) destroy Personal Information whose purpose of processing has been attained or whose retention period has expired.

**7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?**

No, such registration/notification is not required.

**7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?**

Every Controller must prepare and disclose a privacy policy that contains contact information such as the name of the DPO or the name, telephone number, etc. of the department which performs the duties related to Personal Information protection and manages complaints.

## 8 Appointment of Processors

**8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?**

PIPA requires outsourcing of Personal Information Processing to be based on evidencing documents.

**8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?**

The evidencing document for outsourcing must include: i) a requirement that the Personal Information Processing must solely be for the outsourced purpose; ii) technical and managerial safeguards of Personal Information; iii) the purpose and scope of the outsourced work; iv) a restriction against the subcontracting of the outsourced tasks; v) measures to ensure the safety of Personal Information; vi) measures for the supervision of the Outsourcee's management of Personal Information gained in relation to outsourcing; and vii) measures concerning the liability for damages in case of breach of the Outsourcee's obligation.

## 9 Marketing

**9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).**

The Network Act requires express and prior consent of recipients for electronic direct commercial marketing. Consent is not required if someone who has directly collected contact details from a recipient and sold goods or a service to the recipient sends electronic direct marketing for the same kind of goods or service sold within six months of the previous sale. Any electronic direct commercial marketing other than email to be made between 9 p.m. and 8 a.m. of the following day (Korea Standard Time) must obtain separate, prior consent from the intended recipient. It should be noted that there is a detailed regulation on marketing by SMS, such as the form of SMS, reminder of consent, withdrawal process, etc.

**9.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?**

Such restrictions apply to both business-to-business and business-to-consumer marketing.

**9.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).**

Telephone, mobile phone, fax and PC programmes are considered as electronic direct marketing under question 9.1. However, an entity registered as a telemarketer under the Act on Door-To-Door Sales, Etc. may promote over the telephone without the recipient's consent, provided that the source of the recipient's Personal Information is notified by voice.

For non-electronic direct marketing such as marketing by posts, the recipient's prior consent is required under PIPA.

**9.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?**

Such restrictions also apply to marketing sent from other jurisdictions to recipients in Korea.

**9.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?**

The KCC may order corrective action and impose administrative fines on those who have failed to comply with such restrictions, and KISA manages complaints and advises recipients in relation to the transmission of marketing information.

**9.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?**

The lawfulness of sales of marketing lists including Personal Information will be subject to each Data Subject's prior consent. The Data Subject's prior consent will be legitimate if they are notified of the details of such transaction, such as the purpose of the purchaser, the range of Personal Information to be provided, and the retention period of the purchaser.

**9.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?**

Anyone who sends marketing information for a commercial purpose through electronic transmission without express, prior consent from recipients may be subject to an administrative fine of up to 30 million KRW.

## 10 Cookies

**10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).**

Under PIPA, the Controller must disclose its privacy policy, including information about the use of cookies to automatically collect Personal Information, and the means to opt out.

**10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?**

No such distinction is made.

**10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?**

No enforcement action has yet been taken specifically regarding cookies.

**10.4 What are the maximum penalties for breaches of applicable cookie restrictions?**

The collection of cookies without relevant provision in disclosed privacy policy will likely result in an administrative fine of up to 10 million KRW.

## 11 Restrictions on International Data Transfers

**11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.**

If the cause of transfer is outsourcing of a Controller, the Controller is required to post the scope of the outsourced work and the Outsourcee on its homepage. In case of Supply of Personal Information to a foreign third party, the Controller must obtain the Data Subject's prior consent. And consents will be considered improper unless the Controller clearly notifies the details of such Supply, including the receiving third party, the purpose of such third party, the Personal Information to be Supplied, retention period, and the Data Subjects' refusal right and following disadvantages.

However, more strict restrictions apply to ICSP or ICSP-related parties. When ICSP or an ICSP-related party transfers Personal Information abroad, ICSP or the ICSP-elated party should obtain the Data Subjects' consent regardless of the purpose of transfer such as outsourcing, supplying, or storing and establishing protection plans. Information required to be notified to Data Subjects are Personal Information to be transferred, the country, date and method of transfer, the name of the third party and person in charge, Personal Information, the purpose of the third party, and the retention period. However, it is allowed for ICSP or an ICSP-related party to, instead of obtaining a Data Subjects' consent separately, publish or notify those information in privacy policy or via an email in case of transferring for outsourcing or storage.

Notwithstanding the foregoing, an ICSP in a country that restricts cross-border transfer may be subject to an equivalent level of restrictions. However, this will not apply where cross-border transfer is necessary to implement a treaty or other international arrangements.

**11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).**

Please refer to the answer to question 11.1.

**11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.**

No registration/notification is required.

**11.4 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?**

In March 2021, the European Union concluded that South Korea's laws and regulations provide the same level of data protection as the GDPR. PIPC has already issued an order for Personal Information transferred into Korea which will be effective at the date of adequacy decision to supplement the gap or difference between PIPA and GDPR. As Korea is expected be recognised as an adequate country after the *Schrems II* decision in March 2020, the data protection authority is focusing on reflecting the decision in the PIPA amendments rather than issuing any guidelines.

**11.5 What guidance (if any) has/have the data protection authority(ies) issued in relation to the European Commission's revised Standard Contractual Clauses?**

KISA issued guidance on GDPR including conventional

Standard Contractual Clauses in May 2020, but has not updated the guidance yet to reflect the revised Standard Contractual Clauses.

## 12 Whistle-blower Hotlines

**12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?**

Anyone with knowledge that a company has violated or is likely to violate certain laws may report such wrongdoing to the representatives or employees of the company, an administrative agency, an oversight authority with the power to direct, supervise, regulate, or investigate such violation, or an investigative agency, etc., and be protected under the Protection of the Public Interest Reporters Act ("**PPIRA**"). PPIRA only applies when a company has violated or is likely to violate one or more provisions, the violation of which may result in: i) criminal punishment; ii) disposition to withdraw or cancellation of permits, authorisations, or licences granted by a governmental agency; iii) suspension of business; iv) corrective orders; or v) administrative fines, etc. In the case that a report is made, the information of the whistle-blower must be kept confidential, and no disadvantage may be given to the whistle-blower.

**12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?**

In principle, the whistle-blower is to provide: i) his/her Personal Information such as name, resident registration number, address, and contact information; and ii) the identity of the violator of the laws covered by the PPIRA, information about the violation, and purpose and reasons for the report. However, the whistle-blower may remain anonymous by having his/her legal counsel to report *in lieu* of the whistle-blower.

## 13 CCTV

**13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?**

Under PIPA, the installation of CCTV in a public place is permitted only when necessary to: prevent and investigate crime; protect facilities and prevent fire; control traffic; collect, analyse, and provide traffic information; or when specifically permitted by law and no registration, notification, or prior approval from an authority is required for such use of CCTV.

In general, the installer must post a notice detailing: the purpose and place of installation; the range of the cameras' coverage and times of operation; and the name and contact information of the manager in charge.

**13.2 Are there limits on the purposes for which CCTV data may be used?**

Regarding the installation of CCTV in a public place, please refer to the answer to question 13.1.

Regarding the installation of CCTV in a private area, this will be regarded as a means of collecting Personal Information and will usually require the prior consent of Data Subjects.

## 14 Employee Monitoring

**14.1 What types of employee monitoring are permitted (if any), and in what circumstances?**

In general, any employee monitoring that processes the Personal Information of an employee requires the employee's prior consent as a Data Subject under PIPA. Companies typically include the employee's prior written consent in the employment agreement. Further, the Act on the Promotion of Workers' Participation and Cooperation stipulates that a company with 30 or more employees must consult the instalment of employee monitoring tools in the workplace with a labour-management council. Also, the Criminal Act that bans the access to another person's sealed or secretly designed letter, document, or records in all media may be applicable.

It is worth noting a court case where a company removed the hard disk of an employee's personal computer locked by password, connected to another computer and searched using certain keywords. The company did so to verify a rumour that the employee was embezzling the company's funds and found messenger conversations and emails that confirmed the suspicions. The Supreme Court concluded that, under the circumstances – which required urgent and discreet action by the company where: i) it could specifically and rationally suspect that the employee had engaged in a crime; ii) the scope of the access to the hard disk was limited to that related to the crime; iii) the employee agreed when joining the company not to use the company's computer without permission and to return all work-related results to the company; and iv) various materials that confirmed the employee's criminal activity were found as a result of the search – the company's act was justifiable and acceptable in accordance with social norms that were not punishable pursuant to the Criminal Act.

**14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.**

Please see question 14.1.

**14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?**

Please see question 14.1.

## 15 Data Security and Data Breach

**15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?**

Controllers must take the technical, administrative, and physical measures necessary to secure the safety of Personal Information under PIPA. The Outsourcee must also take similar measures, although Controllers also remain liable if damages arise due to an Outsourcee's failure to comply.

**15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

Under PIPA, when the Personal Information of 1,000 or more Data Subjects has been leaked, the Controller must notify the Data Subjects without delay, prepare and take measures to minimise the damage, and report the leak to PIPC or KISA with regard to such notifications and measures. If the Controller is an ICSP or ICSP-related party, such leakage should be reported regardless of the number of Data Subjects and within 24 hours from the time it became aware. The ICSP or ICSP-related party's report should identify the types of Personal Information and the time of such leakage, the measures that can be taken by the Data Subjects, the contact information and more.

**15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

Contrary to the report of the authorities, the Controller must notify the affected Data Subjects of the leakage without delay, regardless of the number of the Data Subjects affected. Such notice shall include the types of Personal Information leaked; the time of the leak; the reason for the leak; the measures that can be taken by the Data Subjects to minimise damages; the countermeasures taken by it and its procedures to remedy the damages to the Data Subjects; and the contact information of its department to which Data Subjects may report any damages incurred by them.

**15.4 What are the maximum penalties for data security breaches?**

The maximum penalties that may be imposed on each entity for a data security breach are as follows:

- Where a Controller fails to take the necessary measures for data security required by PIPA, and Personal Information processed by such Controller has been lost, stolen, leaked, forged, altered or damaged, such Controller may be imprisoned for up to two years or criminally fined up to 20 million KRW.
- Where an ICSP or ICSP-related party fails to take the necessary measures for data security discussed in the answer to question 15.1, and users' Personal Information has been lost, stolen, leaked, forged, altered, or damaged, it may be administratively fined up to 3% of its revenue relating to such violation.
- PIPC may impose and collect fines of up to 500 million KRW if the resident registration number processed by the Controller is lost, stolen, leaked, forged, altered, or damaged.

## 16 Enforcement and Sanctions

**16.1 Describe the enforcement powers of the data protection authority(ies).**

| Investigatory/ Enforcement Power | Civil/Administrative Sanction | Criminal Sanction |
|---|---|---|
| PIPC | PIPC may impose administrative fines or issue corrective orders to the violator of certain provisions of PIPA or other laws relevant to Personal Information protection. | PIPC may refer the violator to certain provisions of PIPA to the public prosecutor. |
| FSC | FSC may impose administrative fines or order the stoppage of business operations for a certain period to the violator of certain provisions of the Credit Information Act. | This is not applicable. |
| KCC | KCC may impose administrative fines or revoke the permission or authorisation granted to a location information provider or a location-based service provider, or order the stoppage of business operations, for a certain period or permanently, if KCC finds non-compliance with certain provisions of the Location Information Act. | This is not applicable. |
| Public Prosecutors | None. | They may prosecute violators of certain provisions of PIPA or other laws related to Personal Information. |

**16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?**

PIPC, FSC and KCC may issue bans to violators of certain provisions related to Personal Information protection, and these bans do not require a court order.

**16.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.**

In Korea, the data protection authorities tend to actively exercise their powers.

For example, in 2019, prior to the revision of the Network Act of 2020, KCC imposed a fine of more than 1.8 billion KRW on an e-commerce company for leaking the Personal Information of only 20 users in 2018, because the company had previously leaked the Personal Information of its users in 2017.

During the three months from January to March 2019, the Ministry of Public Administration and Security, pursuant to PIPA (before its revision in 2020), imposed administrative measures on 91 entities due to violations of PIPA.

**16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?**

KCC administratively fined Google Inc. more than 200 million KRW in 2014, because it had collected the Personal Information of Data Subjects without their prior consent while developing its Street View service. According to KCC's report, KCC personnel visited Google's headquarters in the USA to verify that Google had destroyed the storage disk with the illegally collected data.

## 17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

**17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?**

The Korean legal system does not have a discovery or e-discovery procedure in litigation.

Businesses will typically not cooperate with foreign e-discovery requests or requests for disclosure unless it has substantial impact.

**17.2 What guidance has/have the data protection authority(ies) issued?**

There is no relevant guidance issued by any data protection authority.

## 18 Trends and Developments

**18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.**

In April 2021, PIPC penalised the developer of Iruda, an open-domain conversational AI identified as a 20-year-old female college student. PIPC stated that the developer violated PIPA when using SNS users' chatting logs to teach Iruda.

The developer received the log from other dating application publishers of which privacy policies states that the users are giving consent to use chatting logs to develop new services by logging into the dating applications. PIPA found that the developer used the chatting logs outside the scope of users' consent as users cannot reasonably expect their chatting to be used for development of Iruda and mere log-in is hard to be regarded as consent.

This is the first PIPC's determination on the AI industry and PIPC recently published a personal data checklist for an AI developer and operator.

**18.2 What "hot topics" are currently a focus for the data protection regulator?**

Following last year's large amendment of Personal Information-related legislations, the Korean government is actively leading the update of Personal Information-related legislations to reflect the current and practical demands including the adequacy decision under GDPR.

In January 2021, a Bill to amend PIPA has been announced to collect the public's opinion. The key amendments proposed by the Bill are as follows:

- Cross-border Transfer of Personal Information: The PIPA provisions in relation to cross-border transfer is accused of being confusing as they are separated into general provision and special provision. The Bill organises and upgrades the provisions to have them fit to the global standard. Also, regulation on cross-border transfer of Pseudonymized Information is newly introduced.
- Change of Penalty: Lowers the maximum of criminal penalties to Personal Information leakages and newly adopts administratively fine up to 3% of revenue raised from such leakage. This is to balance the penalty and the interest of the violation and to have PIPA in line with GDPR.
- Transfer Right of Data Subject: The Bill entitles Data Subjects with the right to request a Controller to transfer his/her Personal Information to another Controller.
- Regulations on Mobile CCTV: As the current PIPA only regulates CCTVs fixed at a place, PIPA is to be amended to regulate CCTVs or cameras attached to mobile equipment such as drones or autonomous vehicles.

**Iris Hyejin Hwang** is an associate at D'LIGHT, where she specialises in litigation, local and international dispute resolution related to ICT & new technology, intellectual property, and entertainment & media. Prior to joining D'LIGHT, Ms. Hwang served as a corporate counsel at Neowiz Corporation, where she advised on personal information protection, domestic and international IP licensing, content sourcing, distribution and investment matters relating to PC online/mobile games. Prior to Neowiz, Ms. Hwang was corporate counsel at the Korea Creative Content Agency. She is a dispute resolution expert, having worked on a wide array of local and international litigation and dispute resolution matters involving PC online/mobile games, music and movie industry players in Korea and abroad. Ms. Hwang continues to serve as a mediator at the Korean Commercial Arbitration Board.

**D'Light Law Group**
5F, 311, Gangnam-daero
Seocho-gu
Seoul 06628
Korea

Tel: +82 2 2051 1870
Email: hjh@dlightlaw.com
URL: www.dlightlaw.com/en

**Hye In Lee** is an associate at D'LIGHT, where she focuses on advising and assisting on litigation and legal issues in the ICT and FinTech industries, including blockchain systems. Ms. Lee also has extensive field experience in both international legal cases, such as global investment, M&A and international arbitrations, and local legal cases, including IP litigation, financing, investigations by the public prosecutor and/or the Korean Free Trade Commission, from her time as corporate counsel at Samsung C&T Corporation and Netmarble Corporation.

**D'Light Law Group**
5F, 311, Gangnam-daero
Seocho-gu
Seoul 06628
Korea

Tel: +82 2 2051 1870
Email: hil@dlightlaw.com
URL: www.dlightlaw.com/en

# Mexico


Abraham Diaz Arceo


Gustavo Alcocer

OLIVARES



## 1 Relevant Legislation and Competent Authorities

### 1.1 What is the principal data protection legislation?

The legal framework for data protection is found in Articles 6 and 16 of the Mexican Constitution, as well as in the Federal Law for the Protection of Personal Data Held by Private Parties, published in July 2010, and its Regulations, published in December 2011 (hereinafter the "Law").

### 1.2 Is there any other general legislation that impacts data protection?

Yes. The General Law for the Protection of Personal Data in the Possession of Obliged Subjects, which regulates the processing of personal information in the possession of any Federal, State or local authority (the "Law"); the Privacy Notice Rules, published in January 2013; and the Binding Self-Regulation Parameters, also published in January 2013. It is worth mentioning that Mexican data protection laws and general legislation follow international correlative laws, directives and statutes, and thus have similar principles, regulatory scope and provisions. Moreover, there are other laws such as: the Criminal Code; the Law for the Regulation of Credit Information Companies; the Law for Regulating Financing Technology Institutions; provisions set forth in the Copyright Law and the Federal Law for Consumer Protection; and some specific provisions set forth in the Civil Code and the Commerce Code, which are also related to data protection.

### 1.3 Is there any sector-specific legislation that impacts data protection?

Mexican data protection legislation is not based on sectoral laws. The Law as described above, regulates the collection and processing of any personal information ("PI") by any private entity acting as a Controller or Processor, which impacts any sector that is involved in any sort of personal data collection or processing.

### 1.4 What authority(ies) are responsible for data protection?

The National Institute of Transparency, Access to Information and Personal Data Protection ("INAI") is the authority responsible for overseeing the Law. Its main purpose is the disclosure of governmental activities, budgets and overall public information, as well as the protection of personal data and the individuals' right to privacy. The INAI has the authority to: conduct investigations; review and sanction data protection Controllers; and authorise, oversee and revoke certifying entities.

The Ministry of Economy is responsible for informing and educating on the obligations regarding the protection of personal data between national and international corporations with commercial activities in the Mexican territory. Among other responsibilities, it must issue the relevant guidelines for the content and scope of the Privacy Notice, in cooperation with the INAI.

## 2 Definitions

### 2.1 Please provide the key definitions used in the relevant legislation:

- "**Personal Data**"
  Any information concerning an individual that may be identified or identifiable.
- "**Processing**"
  The collection, use, disclosure or storage of personal data, by any means. The use covers any action of access, management, benefit, storage, transfer or disposal of personal data.
- "**Controller**"
  The individual or private legal entity that determines the processing of personal data or provides the guidelines for the said processing.
- "**Processor**"
  The individual or legal entity that, solely or jointly with another, processes personal data on behalf of the Controller.
- "**Data Subject**"
  Any identified or identifiable natural person.
- "**Sensitive Personal Data**"
  Any personal data that may affect the most intimate sphere of an individual, or that which, if misused, may lead to discrimination or carry a serious risk to the individual. In particular, sensitive personal data are considered those that may reveal information such as ethnic or racial origin, a present or future medical condition, genetic information, religious, philosophical and moral beliefs, union affiliation, political opinions and sexual preference.
- "**Data Breach**"
  Data Breach means any security breach that if occurring in any phase of the data collection, storage or use, may affect in a significant manner the patrimonial or moral rights of individuals.
- "**ARCO rights**"
  Refers to the access, rectification, cancellation or opposition rights, which can be enforced by any data subject, in connection with the collecting or processing of its personal information.

- "**Consent**"
  An expression of will made by any data subject, or by any person with legal authority to act on behalf of the data subject, for conducting any activity related to the collecting or processing of the personal information of the data subject.
- "**Pseudonymisation**"
  The processing of personal data in such a manner that it can no longer be attributed to a specific data subject, without the use of additional information.
- "**Privacy Notice**"
  A document issued by the Controller either in physical, electronic or any other format, which is made available to the data subject prior to processing his/her personal data, and whereby the Controller informs the data subject, among other matters, about: the terms for the collection of personal data; which personal information will be collected; the identity of the Controller; the purpose of the data collection; the possible transfers of data; and the mechanisms for the data subject to enforce its ARCO rights.
- "**Transfer**"
  Any data communication made to a person other than the Collector or the Processor, either in Mexican territory or abroad.

## 3 Territorial Scope

### 3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

Mexican data protection law is not limited to PII Controllers established or operating in Mexican territory. Although the Law does not provide a specific reach or scope of its applicability, the Regulations to the Law do. In this regard, such regulations (and, therefore, the Law), in addition to being applicable to companies established or operating under Mexican law (whether or not located in Mexican territory) apply to companies not established under Mexican law that are subject to Mexican legislation derived from the execution of a contract or under the terms of international law.

Additionally, Mexican regulations on data protection apply to: company establishments located in Mexican territory; persons or entities not established in Mexican territory but using means located in such territory, unless such means are used merely for transition purposes that do not imply a processing or handling of personal data; and when the Controller is not established in Mexican territory but the person designated as the party in charge of the control and management of its personal data (a service provider) is.

In the case of individuals, the establishment will mean the location of the main place of business or location customarily used to perform their activities or their home.

## 4 Key Principles

### 4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  This principle is not defined in the Law; however, the Law makes it clear that personal data can in no way be collected, stored or used through deceitful or fraudulent means.
- **Lawful basis for processing**
  The Controller is responsible for processing personal and/or sensitive data in accordance with the principles set forth in the Law and international treaties.
- **Purpose limitation**
  Personal data shall only be collected and processed in compliance with the purpose or purposes set forth in the Privacy Notice. Moreover, the purpose of the Privacy Notice must be certain, which is achieved by establishing the purpose for which the personal data will be collected and processed in a clear, objective manner, not leaving any room for confusion.
- **Data minimisation**
  The Controller will be responsible and shall endeavour to make reasonable efforts so that the personal data processed are the minimum necessary, according to the purpose that originated the collection of PI.
- **Proportionality**
  Controllers can only collect personal data that are necessary, appropriate and relevant for the purpose(s) of their collection.
- **Retention**
  This translates into the obligation of the Controller to retain personal data only for the period of time necessary for complying with the purpose(s) for which the data were collected, with the obligation to block, cancel and suppress the personal data afterwards.
- "**Responsibility**"
  The Controller must safeguard and be accountable for any PI under its custody, or any PI that it has shared with any vendor, either in Mexico or abroad. In order to comply with this principle, the Controller must make use of any of the best international practices, corporate policies, self-regulatory schemes or any other suitable mechanism to this effect.
- "**Quality**"
  This principle is accomplished when the personal data processed are accurate, complete, pertinent, correct and updated as required, in order to comply with the purpose for which the personal data will be collected.
- "**Consent**"
  The Controller shall obtain the consent of the data subject, prior to the collection of any personal information, and must keep evidence of the consent.
- "**Loyalty**"
  This consists of the obligation of the Controller to process any PI collected favouring the protection of the interests of the data subject and the reasonable expectation of privacy.

## 5 Individual Rights

### 5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**
  Data subjects have the right to access their personal data held by the Controller at any time they request.
- **Right to rectification of errors**
  Data subjects have the right to request the rectification of any of their personal data, held by a Controller, which turns out to be inaccurate, incomplete or out of date.
- **Right to deletion/right to be forgotten**
  Data subjects have the right to request the cancellation of their personal data. The cancellation of personal data will result in a blocking period, after which the suppression of the data will take place. Notwithstanding the foregoing, the Controller may keep such personal data exclusively for the purposes of the responsibilities regarding their treatment. Likewise, the Law establishes some cases where the Controller is not obliged to cancel or delete the personal data.

- **Right to object to processing**
  Data subjects have the right to object to the processing of their personal data due to a legitimate reason.
- **Right to restrict processing**
  Data subjects have the right to restrict the processing of their personal data due to a legitimate reason.
- **Right to data portability**
  Data subjects have the right to obtain, from the subject concerned, a copy of his/her processed data, which allows the data subject to continue using his/her personal information.
- **Right to withdraw consent**
  At any time, the data subject may withdraw his/her consent for the treatment of his/her personal data. The Controller must establish simple and free mechanisms that allow the data subjects to withdraw their consent at least by the same means by which they granted it.
- **Right to object to marketing**
  In addition to the general rights described above, data subjects have the right to oppose the use of their personal data for marketing or advertising purposes.
- **Right to complain to the relevant data protection authority(ies)**
  Data subjects are entitled to submit a claim before the INAI. The claim must be filed in writing and shall clearly state the provisions of the Law that are deemed infringed; also, it must be submitted within the 15 days following the date on which the response to the data subject has been communicated by the Controller.
- **Right to a verification procedure**
  Data subjects have the right to request before the INAI, a verification procedure, by which the authority will check the Controller's compliance with all the provisions set forth in the Law, or any other applicable regulations.

## 6 Registration Formalities and Prior Approval

**6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?**

No, there is not.

**6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?**

This is not applicable.

**6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?**

This is not applicable.

**6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?**

This is not applicable.

**6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?**

This is not applicable.

**6.6 What are the sanctions for failure to register/notify where required?**

This is not applicable.

**6.7 What is the fee per registration/notification (if applicable)?**

This is not applicable.

**6.8 How frequently must registrations/notifications be renewed (if applicable)?**

This is not applicable.

**6.9 Is any prior approval required from the data protection regulator?**

This is not applicable.

**6.10 Can the registration/notification be completed online?**

This is not applicable.

**6.11 Is there a publicly available list of completed registrations/notifications?**

This is not applicable.

**6.12 How long does a typical registration/notification process take?**

This is not applicable.

## 7 Appointment of a Data Protection Officer

**7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.**

The appointment of a Data Protection Officer (person or department) by the Controller is mandatory.

**7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?**

Failure to appoint a Data Protection Officer (person or department) is not expressly catalogued as an infringement in the Law. However, Section XIX of Article 63 of the FLPPDHPP contains a "catch all" provision that considers as an infringement any failure to comply with the obligations set forth in the Law. Therefore,

failure to appoint a DPO has to be deemed an administrative infringement. Nevertheless, there is no express sanction in the law for the infringements referred to in Section XIX above.

**7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?**

No, they are not.

**7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?**

Yes, it can.

**7.5 Please describe any specific qualifications for the Data Protection Officer required by law.**

There are no statutory requirements. Notwithstanding the foregoing, it is recommended to appoint a person, team or department with at least the following qualifications: i) data privacy expertise (certification desired); and ii) enough authority and resources to advocate and implement measures in order to protect the personal data within the company.

**7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?**

The responsibilities of a Data Protection Officer required by law are to: i) process all claims related to the enforcement of ARCO rights; and ii) foster and enhance the protection of personal data inside the company.

**7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?**

No, there is no statutory obligation to register or notify the appointment of a Data Protection Officer to any authority.

**7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?**

It is necessary to mention in the Privacy Notice the name and domicile (contact information) of the person or department that will be responsible for the collection, use and storage of the personal data.

## 8 Appointment of Processors

**8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?**

Yes, the relationship between the business and the Processor must be established by means of contractual clauses or other legal instruments determined by the business; and it is necessary to prove the existence, scope and content of the relationship.

**8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?**

The agreement shall be in writing and signed by both parties. The agreement shall contain at least the following obligations on the Processor: i) to treat only personal data according to the instructions of the business; ii) to treat only personal data for the purposes instructed by the business; iii) to implement security measures in accordance with the Law, and other applicable provisions; iv) to keep confidentiality regarding the personal data processed; v) to delete all PI processed once the legal relationship with the business is over, or when the instructions of the business have been fulfilled, provided that there is no legal provision that requires the preservation of the personal data; and vi) to refrain from transferring PI unless the business determines so, or when it is required by a competent authority. It is worth mentioning that agreements between the business and the Processor in relation to the treatment of personal data must be in accordance with the corresponding Privacy Notice.

## 9 Marketing

**9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).**

Mexico does not have any specific regulations dealing with unsolicited text messages or spam emails, but the Federal Bureau for Consumer Protection operates a call-blocking registry ("REPEP"), covering both landlines and mobile phone numbers, which gives suppliers 30 days making marketing calls, sending marketing messages and to stop disturbing the consumer at his/her registered address, electronic address, or by any other means. Likewise, all the marketing purposes have to be specified clearly in the Privacy Notice.

**9.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?**

Please refer to question 9.1 above.

**9.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).**

Please refer to question 9.1 above.

**9.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?**

Please refer to question 9.1 above.

**9.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?**

Issues regarding marketing restrictions are regularly addressed by the Federal Bureau for Consumer Protection.

**9.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?**

Since Mexican law expressly provides that the collecting or processing of any personal information has to be through lawful means, the purchasing of marketing lists, including any personal information not collected in accordance with Mexican law, would not be deemed legal. If the marketing list includes only business contact information or publicly available information, then it can be used, and it is always recommended to provide recipients of emails sent for marketing purposes with a mechanism that allows an easy opt-out from the marketing service.

**9.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?**

According to the Federal Consumer Protection Law, the maximum penalties for marketing breaches may reach the amount of MXN$1,858,189.39 (approximately US$89,535.00).

## 10 Cookies

**10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).**

The Guidelines for drawing up the Privacy Notice require: individuals be informed as to any technology that allows the automatic collection of PI simultaneously with the first contact with the individuals; data owners request consent from individuals through an opt-in mechanism; and individuals be informed as to how to deactivate said technology, unless said technology is required for technical reasons.

**10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?**

No, they do not.

**10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?**

No, they do not.

**10.4 What are the maximum penalties for breaches of applicable cookie restrictions?**

Although there is not any express infringement regulated in the Law in connection with the use of cookies, their use in contravention to the Guidelines mentioned above would translate to an illicit collecting of PI, which would be sanctioned with a fine of up to US$1,500,000, and if the infringement persists, an additional fine of up to US$1,500,000 may be imposed.

## 11 Restrictions on International Data Transfers

**11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.**

If the Controller is willing to transfer any PI to any third parties, either domestic or foreign, it needs to obtain the informed consent of data subjects for the said data transfer, in advance, through the corresponding Privacy Notice. There are some cases where third parties do not require the consent of the data subject for the transfer of PI. According to Article 37 of the Law, consent will not be necessary only in the following cases:

i) when expressly allowed by the Law;
ii) when PI is available in publicly accessible sources;
iii) when personal data has been dissociated;
iv) when the collection of personal data is needed for compliance with obligations derived from a legal relationship between the data subject and the data owner;
v) when there is an emergency situation that jeopardises the person or the commodities of the data subject; and
vi) when the collection of PI is indispensable for medical attention and/or diagnosis; for rendering sanitary assistance; for medical treatment or sanitary services; provided that the data subject is not in a condition to give consent; and provided that the data collection is performed by a person subject to legal professional privilege.

**11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).**

As stated above, according to Article 36 of the Law, if any Controller is willing to transfer any PI to third parties, either domestic or foreign, it must obtain consent from the data subject in advance, through a Privacy Notice. When the transfer is performed, the vendor or third party will be obliged in exactly the same terms as the Controller, by means of an agreement that has to be executed in writing.

**11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.**

There is no registration/notification requirement set forth in the Law for data transfers.

**11.4 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?**

There has been no guidance from the Mexican DPA following the decision of the Court of Justice of the EU in *Schrems II* (Case-311/18).

**11.5 What guidance (if any) has/have the data protection authority(ies) issued in relation to the European Commission's revised Standard Contractual Clauses?**

There has been no guidance from the Mexican DPA issued in relation to the European Commission's revised SCC's.

## 12 Whistle-blower Hotlines

**12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?**

Whistle-blower hotlines can be put into operation, but the Law is silent as to any restrictions on the personal data that may be processed through them.

**12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?**

Anonymous and non-anonymous reporting is allowed.

## 13 CCTV

**13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?**

There is no registration or notification requirement for the use of CCTV.

**13.2 Are there limits on the purposes for which CCTV data may be used?**

The Law is silent as to the limits on the purposes for which CCTV data may be used.

## 14 Employee Monitoring

**14.1 What types of employee monitoring are permitted (if any), and in what circumstances?**

In January 2021, there was an amendment to Mexican Federal Labor Law, introducing the regulation of "Telework", thus establishing the right of employers to monitor employee's activities working under this modality, and the obligation of employees to use the technology provided by employers in order to monitor the activities carried out under the modality of telework.

The monitoring of the employee is limited to the activities carried out under the modality of telework, and this amendment also recognises the right of employees to "disconnect", whenever they are not performing their work, in order to respect their privacy.

This amendment only established a general legal frame that will have to be detailed in the years to come.

The general rules set forth by this amendment will also have to be interpreted by the Mexican Courts on a case-by-case basis, in order to generate jurisprudence in this regard.

**14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.**

A written agreement will have to be executed between the employer and employees working under the modality of telework, and in said agreement the consent to be monitored during working hours will have to be collected.

Also, since the collection, storage and use of any audio or video material featuring the voice and image of any individual within the workplace may be deemed a collection of PI, employers are required to give employees notice as to the use of video surveillance technology at workplaces.

Mexican DPA has drawn up a short model Privacy Notice to be used by any individual or company introducing video surveillance technology on their premises.

Said summary Privacy Notice must be visible at the entrance to monitored spaces, and must inform individuals of the purpose of the surveillance and the treatment of the collected information.

**14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?**

Currently, it is not mandatory to consult or notify employee's representatives at works councils/trade unions. However, in light of the above-mentioned amendment, it may change in the near future, when negotiating collective labour agreements for employees working under the modality of telework.

## 15 Data Security and Data Breach

**15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?**

Article 19 of the Federal Law for the Protection of Personal Data Held by Private Entities requires every Controller to implement and maintain administrative, technical and physical security measures, which protect the collected and stored PI from any loss, alteration, destruction or from any unauthorised access and use.

Said measures cannot be lesser than those used by the data owner to protect its own information. For their implementation, the data owner must consider the existing risk and the possible consequences for the data subjects, the sensitivity of the data, and technological developments. Therefore, security measures may vary from industry to industry, and from company to company.

**15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

There is no legal requirement to report data breaches to the INAI, and so far, there are no guidelines for voluntary breach reporting to the INAI.

**15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

Mexican law sets forth that if any phase of collection, storage or use of data "may in any way affect in a significant manner the patrimonial or moral rights of individuals", data owners shall immediately notify individuals about this situation.

However, so far there is no further explanation in the law or in the jurisprudence, as to what is to be deemed a significant effect on the patrimonial or moral rights of data subjects.

Likewise, Article 64 of the Regulations of the Law requires data owners to notify individuals, without any delay, as to any breach that significantly affects their moral or patrimonial rights, as soon as the data owner confirms that a breach has occurred, and when the data owner has taken any actions towards starting an exhaustive process to determine the magnitude of the breach.

In said notification, data owners must state at least:

- the nature of the incident;
- the compromised PI;
- recommendations for the data subjects to protect their interests;
- the corrective measures immediately implemented by the data owner; and
- the means of obtaining more information regarding the breach.

**15.4 What are the maximum penalties for data security breaches?**

According to the Federal Consumer Protection Law, the penalties for data security breaches regarding marketing matters are up to MXN$1,858,189.39 (approximately US$89,535.00).

If Mexican DPA determines that a data breach is attributable to a Controller or Processor, a fine of up to MXN$320,000 in minimum wage) (approximately US$1,400,000) may be imposed.

## 16 Enforcement and Sanctions

**16.1 Describe the enforcement powers of the data protection authority(ies).**

(a) **Investigative Powers**: Verification Proceeding: the INAI is entitled to conduct inspections *ex officio* at any company, in order to determine its compliance with the legislation on PI.

(b) **Corrective Powers**: The INAI is entitled to declare administrative infringements in order to enforce the ARCO rights of any individual, for omitting in the Privacy Notice, any or all of the elements established in Law, collecting or transferring personal data without the express consent of the holder, for obstructing the authority's acts of verification, for violating the security of databases, programs or equipment, when it is attributable to the responsible party, among others.

(c) **Authorisation and Advisory Powers**: The INAI is entitled to develop, promote and disseminate analyses, studies and research on the protection of personal data held by private parties and to provide training to regulated entities. It may also provide technical support to those responsible, upon request, for compliance with the obligations established in the Law.

(d) **Imposition of administrative fines for infringements of specified GDPR provisions**: The INAI is entitled to declare administrative infringements and impose administrative fines for non-compliance with any of the principles or provisions of the Law.

**16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?**

This authority is not expressly designated in the Law as the INAI. However, considering that the Law recognises the INAI as the specialised authority in charge of the protection of PI in Mexico, the INAI should be deemed as having the authority to ban a particular processing activity. However, if contested by any third party, any ban issued by the INAI should be validated by the Mexican Federal Administrative Courts.

**16.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.**

There are no recent cases or precedents illustrating this authority's approach.

**16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?**

So far there is no precedent of Mexican DPA having exercised its powers against businesses established in other jurisdictions.

## 17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

**17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?**

Any e-discovery requests or requests for disclosure from foreign law enforcement agencies have to be validated by Mexican Courts, in order that they may be validly enforced in Mexico. If any order or request from any foreign law enforcement agency is not validated through a Mexican Court, a company may refuse to comply with it.

**17.2 What guidance has/have the data protection authority(ies) issued?**

In connection with e-discovery and disclosure to foreign law enforcement agencies, no guidance has been issued by the INAI.

## 18 Trends and Developments

**18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.**

There are no enforcement trends which have emerged during the previous 12 months from Mexican DPA (INAI).

### 18.2 What "hot topics" are currently a focus for the data protection regulator?

As a result of the COVID-19 pandemic, e-commerce and telework are growing exponentially in Mexico, thus becoming the main focus for data protection regulators. Some bills are being passed to the Congress in order to improve the legal framework in connection with the regulation of e-commerce and social media, which may have an indirect impact on the protection of personal data. However, currently there is no bill being studied in order to modify the FLPPDHPE.

Furthermore, the Mexican data protection regulator is looking forward to joining Convention 108+, which should improve the protection of personal data in Mexico and may trigger an amendment to the FLPPDHPE.

**Abraham Diaz Arceo** co-chairs OLIVARES' Privacy and IT Industry groups and has a wealth of knowledge across all areas of intellectual property (IP), with a focus on litigation, copyright, right of publicity, trademarks, unfair competition, licensing, prosecution and opposition matters. He also handles domain disputes under the Uniform Domain Name Dispute Resolution Policy (UDRP) and the Local Dispute Resolution Policy (LDRP) and provides strategic advice on website development, protection of website content, online advertisement, and compliance on e-commerce and privacy law regulations. Mr. Diaz has authored articles on IP and Internet matters, as well as on privacy law, for leading industry publications and has lectured on cutting-edge IP topics in national and international fora. His representative cases include defence of the producers of the documentary film, *Presunto Culpable,* from various civil law suits filed by individuals portrayed in the documentary, which set the basis for regulations now applicable to the documentary film industry in connection with the use of a person's image.

**OLIVARES**
Pedro Luis Ogazon 17
San Angel, 01000
Mexico City
Mexico

Tel: +52 55 532 23041
Email: abraham.diaz@olivares.mx
URL: www.olivares.com.mx

**Gustavo Alcocer** manages the Corporate and Commercial Law Group at OLIVARES, advising domestic and foreign businesses and the owners of those businesses on Mexico and cross-border corporate and commercial transactions. He serves as outside general counsel in Mexico to many of his domestic and foreign clients and has significant experience in domestic and cross-border transactions. With more than 30 years of law firm and in-house practice experience, Mr. Alcocer possesses a wealth of transactional knowledge in M&A, finance, and business law and advises clients across IP-intensive industry sectors such as life sciences, information technology, food and beverage, transportation, and retail. Clients routinely turn to him for sophisticated strategic advice regarding structuring, maintaining and expanding operations in Mexico, as well as on valuation and monetisation.

**OLIVARES**
Pedro Luis Ogazon 17
San Angel, 01000
Mexico City
Mexico

Tel: +52 55 532 23000
Email: gustavo.alcocer@olivares.mx
URL: www.olivares.com.mx

# Morocco

Hajji & Associés

Ayoub Berdai

## 1 Relevant Legislation and Competent Authorities

### 1.1 What is the principal data protection legislation?

The principle data protection legislation in Morocco is as follows:

- Article 24 of the Constitution of Morocco;
- Law No. 09-08 on the Protection of Individuals with Regard to Processing of Personal Data (the "**Data Protection Law**");
- Decree No. 2-09-165 issued for the implementation of Law Data Protection Law;
- Prime Ministerial Decree No. 3-33-11 approving the Internal Regulations of the National Commission for the Protection of Personal Data ("**CNDP**"); and
- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108).

### 1.2 Is there any other general legislation that impacts data protection?

The General Data Protection Regulation (EU) 2016/679 ("**GDPR**") could, according to its extraterritorial scope (article 3), be applied to the Moroccan entities that collect and process of Data Subject's personal data located in the European Union.

### 1.3 Is there any sector-specific legislation that impacts data protection?

The Moroccan Regulator Authority, or in French, the *Commission Nationale de contrôle de la protection des Données à caractère Personnel* (the "**CNDP**"), has issued guidelines on data protection-related matters, in particular:

- Resolution No. D-188-2020 as of December 12, 2020 relating to the data protection impact assessment;
- Resolution No. 465-2013 as of September 6, 2013 establishing the list of States ensuring adequate protection of privacy and fundamental rights and freedoms of individuals with regard to the processing of personal data;
- Resolution No. 98-AU-2015 as of June 12, 2015 on the model request for standard authorisation with regard to the processing of the supplier's personal data;
- Resolution No. 32-2015 as of February 13, 2015 on the model declaration in respect of the processing of customers' personal data;
- Resolution No. 508-AU-2014 as of November 14, 2014 on the model declaration in respect of the processing of personal data relating to online sales; and
- Resolution No. 298-AU-2014 as of April 11, 2014 on the model request for standard authorisation in respect of the processing of personal data implemented by the private sector or assimilated via Human Resources.

### 1.4 What authority(ies) are responsible for data protection?

The authority responsible for data protection is the CNDP which is based in Rabat, Morocco.

## 2 Definitions

### 2.1 Please provide the key definitions used in the relevant legislation:

- "**Personal Data**"
  Personal Data "*données à caractère personnel*" means any information regardless of their nature and format, relating to an identified or identifiable natural person "the **Data Subject**". An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- "**Processing**"
  Processing of Personal Data "*traitement de données à caractère personnel*" means any operation or set of operations that is performed on personal data, whether or not by automated means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- "**Controller**"
  The Data Controller "*Responsable du traitement*" is the natural or legal person, public authority, agency or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data.
- "**Processor**"
  The Data Processor "*sous-traitant*" is the natural or legal person, public authority, agency or other body that processes personal data on behalf of the Controller.
- "**Data Subject**"
  Data Subject "*Personne concernée*" is the natural person who is the subject of the relevant personal data.
- "**Sensitive Personal Data**"
  Sensitive Personal Data "*données sensibles*" means personal

data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership or which concern health and genetics.

- "**Data Breach**"
  Data Breach "*violation de données à caractère personnel*" is defined by the GDPR as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
- **Third Party**
  "**Third party**" "*Tiers*" is the natural or legal person, public authority, agency or body other than the Data Subject, Controller, processor and persons who, under the direct authority of the Controller or processor, are authorised to process personal data.
- **Recipient**
  Recipient "*Destinataire*" is the natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, the bodies that may receive Personal Data in respect of a particular legal provision shall not be considered as Recipients, in particular the CNDP.
- **Consent of the Data Subject**
  Consent of the Data Subject "*Consentement de la personne concernée*" means any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which she signifies agreement to the processing of its Personal Data.

## 3 Territorial Scope

### 3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The Data Protection Law applies when the Controller is not established on Moroccan territory but uses, for the purpose of processing Personal Data, automated means or not, located on Moroccan territory, with the exception of processing that is used only for the purpose of transit on the Moroccan territory or on that of a State whose legislation is recognised as equivalent to that of Morocco in respect of the protection of Personal Data.

## 4 Key Principles

### 4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  Article 5 *et seq.* of the Data Protection Law provides that the Controllers should provide certain minimum information to Data Subjects regarding the collection and further processing of their Personal Data. Such information must be provided in a concise and unequivocal manner.
- **Lawful basis for processing**
  The Personal Data should be processed fairly and lawfully. The processing of Personal Data is lawful only if, and to the extent that, it is permitted under the Data Protection Law, which provides the following exhaustive list of legal basis on which Personal Data may be processed:
  i. prior, freely given, specific, informed and unambiguous consent of the Data Subject;
  ii. compliance with legal obligations to which the Controller or the Data Subject are subject;
  iii. public interest;
  iv. contractual necessity, i.e., for the performance of a contract to which the Data Subject is a party, or for the purposes of pre-contractual measures taken at the Data Subject's request; or
  v. legitimate interests pursued by the Controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject. In such situation, a legitimate interest assessment could be requested by the CNDP.

  In practice, the CNDP requests a detailed documentation and is more vigilant when a Controller does not provide proof of the Data Subject's consent and claims a legitimate interest or other grounds of legal bases for data processing.
- **Purpose limitation**
  Personal Data should only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes. The use of Personal Data in a manner that is incompatible with the purposes for which they were initially collected is subject to the prior consent of the Data Subject and the prior authorisation of the CNDP.
- **Data minimisation**
  Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are collected and processed.
- **Proportionality**
  The Resolution No. D-188-2020 as of December 12, 2020 relating to the data protection impact assessment provides that the processing of Personal Data should be proportional and limited to the minimum necessary to carry out the processing purpose.
- **Retention**
  Personal Data must be kept in a form that permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed.

## 5 Individual Rights

### 5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right to information**
  The Data Subject should be informed beforehand of any processing in an express, precise and unequivocal manner by the Controller of the following:
  i. the identity and the contact details of the Controller and, where applicable, of the Controller's representative;
  ii. the purposes of the processing;
  iii. the Recipients of the Personal Data, if any;
  iv. where applicable, if there is any transfer of Personal Data abroad;
  v. the existence of the right (a) of access to Personal Data, (b) of rectification of errors, and (c) to object to the processing of such data;
  vi. whether the Data Subject is required to provide its Personal Data and of the possible consequences of failure to provide such data; and
  vii. the characteristics of the CNDP's receipt of the Controller's declaration or of the CNDP's authorisation.

  The Data Protection Law provides some exceptions to the principle described above. In particular, the right to information is not applicable (i) when it proves impossible to inform the Data Subject, (ii) to collect and process Personal Data necessary for national or

international security, (iii) if a particular legislation expressly provides for the recording or communication of Personal Data, and (iv) to the processing of Personal Data carried out exclusively for journalistic, artistic or literary purposes.

- **Right of access to data/copies of data**
  The Data Subject shall have the right to request from the Controller, at reasonable intervals – without delay and free of charge – the following:
  i. the confirmation as to whether or not its Personal Data are being processed, the purposes of the processing, the categories of Personal Data concerned by such processing and the Recipients or categories of Recipient to whom the Personal Data have been or will be disclosed;
  ii. a copy of the Personal Data being processed as well as any available information on the origin of this data; and
  iii. the existence of automated decision-making and the meaningful information about the logic involved in such processing.

  It should be noted that the Controller has the right to request from the CNDP time limits for responding to legitimate requests of access and may object to requests that are manifestly abusive, in particular because of their number and repetitive nature. In the event of opposition by the Controller, the burden of proof of manifestly abusive nature shall lie with the latter.
- **Right to rectification of errors**
  The Data Subject shall have the right to obtain from the Controller free of charge and within 10 days at the latest, the rectification of its inaccurate Personal Data.
  In the event of refusal or failure to reply within the above-mentioned time limit, the Data Subject may submit a request for rectification to the CNDP, which shall instruct one of its members to carry out all useful investigations and have the necessary rectifications made as soon as possible.
- **Right to deletion/right to be forgotten**
  The Data Subject shall have the right to obtain from the Controller free of charge and within 10 days at latest, the erasure of Personal Data whose processing does not comply with the provisions of the Data Protection Law.
- **Right to object to processing**
  The Data Subject shall have the right to object, on legitimate grounds, to the processing of its Personal Data. Where Personal Data are processed for direct marketing purposes, the Data Subject shall have the right to object at any time to processing of its Personal Data concerning such marketing activities.
- **Right to withdraw consent**
  The Data Subject has the right to withdraw its consent at any time. It is important to underline that the withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal.
- **Right to object to marketing**
  The Data subject have the right to object to the processing of personal data for the purpose of direct marketing.
- **Right to complain to the relevant data protection authority(ies)**
  The Data Subject has the right to lodge complaints with the CNDP concerning the processing of its Personal Data either by (i) registered letter, (ii) hand delivering a letter to the CNDP's secretariat, or (iii) by online filing (https://www.cndp.ma/fr/service-en-ligne/personnes-concernees/plainte-en-ligne.html).

A complaint template has been published by the CNDP on its website (https://www.cndp.ma/fr/service-en-ligne/personnes-concernees/modeles-de-courrier.html).

## 6 Registration Formalities and Prior Approval

### 6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

The Controller that wishes to collect and process Personal Data is required to submit either a declaration or an authorisation request to the CNDP depending on the sensitivity of the data. Such a procedure should necessarily be carried out before any collection and processing of Personal Data.

Thus, the Controller should notify the CNDP by carrying out the appropriate procedure, namely:

1. **A request for authorisation:**
   i. if there is a collection and processing of Sensitive Data;
   ii. if there is a change of the initial declared purpose, i.e. the Personal Data is used for purposes other than those for which it was collected;
   iii. if the data processing relates to offences, condemnations or security measures;
   iv. if there is a collection and processing of the Data Subject's identity card number; and
   v. if the processing requires the interconnection of files with different purposes.
2. **A prior declaration:**
   The prior declaration to the CNDP is required whenever the prior authorisation is not ordered by the Data Protection Law.

### 6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

Yes. The authorisation/declaration application are very specific and should specify some accurate information including but not limited to: the Controller's details; the main characteristics of the processing; the Personal Data to be processed; and the retention period of the processed data.

Any type of data to be processed, e.g. HR data, CCTV, customer's data etc., should be subject to a specific authorisation/declaration application.

### 6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

The application to the CNDP is made generally (i) either according to the Controller's identity, (ii) or to the Personal Data category and processing purposes.

### 6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

The registration requirements are applicable to:

i. the Controllers established on the Moroccan territory; and

ii. the Controllers not established on the Moroccan territory but which use, for the purpose of processing personal data, automated means or not, located on Moroccan territory.

### 6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

The information to be included on the authorisation/declaration application depends on the categories of Personal Data to be processed. The authorisation/declaration form should particularly specify the following information:

i. the Controller's identity;
ii. the legal basis on which Personal Data may be processed;
iii. the category of the data;
iv. the identification of the Controller's representant, if any;
v. the identification of the Processor of the Third Party, if any;
vi. the processing purpose;
vii. the transfer of data abroad, if any; and
viii. the security measures implemented to preserve the security and confidentiality of data.

### 6.6 What are the sanctions for failure to register/notify where required?

According to the article 52 of the Data Protection Law, the implementation of a Personal Data file without the requested prior declaration or authorisation is punished with a fine of MAD 10,000 (approx. USD 1,120) to MAD 100,000 (approx. USD 11,200).

Moreover, when the perpetrator is a legal entity, the fine described above can be doubled. The legal entity may in addition be subject to (i) a partial forfeiture of its properties, or (ii) the closure of its premise(s) where the offence was committed.

### 6.7 What is the fee per registration/notification (if applicable)?

The procedure before the CNDP is free of charge.

### 6.8 How frequently must registrations/notifications be renewed (if applicable)?

This is not applicable.

### 6.9 Is any prior approval required from the data protection regulator?

Please refer to the answer to question 6.1.

### 6.10 Can the registration/notification be completed online?

The declaration and authorisation application are notified to the CNDP by (i) registered letter, (ii) hand-delivering a letter to the CNDP secretariat, or (iii) electronic means such as acknowledgment of receipt received by email.

### 6.11 Is there a publicly available list of completed registrations/notifications?

There is no publicly available list in respect of the completed declaration and/or authorisation granted by the CNDP.

### 6.12 How long does a typical registration/notification process take?

The timeframes for the processing of applications of declarations and authorisations by the CNDP are as follows:

**i. For a declaration:**

The CNDP shall issue, within 24 hours from the date of acknowledgment of the declaration's application, a receipt for the said declaration. The Controller may implement the processing of data upon issuance of the said receipt.

However, where it appears to the CNDP, upon examination of the declaration's application, that the processing envisaged by the Controller presents clear dangers for the respect and protection of privacy and of the fundamental rights and freedoms of individuals with regard to the processing to which such data are or may be subject, the CNDP shall decide to subject the said processing to the prior authorisation regime as explained above.

The CNDP's motivated decision shall be notified to the Controller within eight days of the application being filed.

**ii. For a prior authorisation:**

The CNDP shall give its decision within two months from the date of receipt of the authorisation's application. This time limit may be extended once. However, if the file is incomplete, the Controller is informed and the time limit starts when the requested information or document are provided.

It should be noted that when the CNDP has not taken a decision within the aforementioned period, i.e. four months, the authorisation is deemed to have been granted.

## 7 Appointment of a Data Protection Officer

### 7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

Neither the Data Protection Law nor the CNDP deals with the appointment of a Data Protection Officer. The legal status of the Data Protection Officer could be incorporated in the future Moroccan law on personal data that is currently under preparation.

It should be noted that the Moroccan companies subject to the GDPR provisions should comply with the obligations prescribed by the article 37 *et seq.* of the GDPR relating to the designation of a Data Protection Officer.

### 7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

This is not applicable.

**7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?**

This is not applicable.

**7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?**

This is not applicable.

**7.5 Please describe any specific qualifications for the Data Protection Officer required by law.**

This is not applicable.

**7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?**

This is not applicable.

**7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?**

This is not applicable.

**7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?**

This is not applicable.

## 8 Appointment of Processors

**8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?**

Yes. The Controller that appoints a Processor in order to process Personal Data on its behalf is required to enter into a binding agreement with the said Processor.

Besides, it is important to note that the Controller should choose a Processor who provides sufficient guarantees with regard to the technical and organisational security measures relating to the processing to be carried out and must ensure compliance with these measures.

**8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?**

The relationship between the Controller and the Processor should be governed by a written agreement binding the parties and stipulating, in particular, that the Processor acts only under the sole instructions of the Controller and that the processor should implement the appropriate technical and organisational measures to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access and against any other form of unlawful processing.

In practice, the agreement's terms stipulate that the processor:

i. only acts on the Controller's instructions;
ii. imposes confidentiality obligations on its employees;
iii. ensures the security of Personal Data that it processes;
iv. abides by the rules of regarding the appointment of sub-processors;
v. implements measures to assist the Controller with guaranteeing the rights of Data Subjects;
vi. assists the Controller in obtaining approval from the CNDP;
vii. either returns or destroys the Personal Data at the end of the relationship; and
viii. provides the Controller with all information necessary to demonstrate compliance with the Data Protection Law and allows for and contributes to audits, including inspections, conducted by the Controller or the CNDP.

## 9 Marketing

**9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).**

Pursuant to article 10 of the Data Protection Law, the transmission of electronic communications for purposes of direct marketing shall be permissible only with the prior consent ("opt-in") of the Data Subject. However, prior consent to the email direct marketing is not required for Data Subjects who have already purchased similar products or services.

Furthermore, the Data Subject should have the right to object at any time to receiving marketing communication.

**9.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?**

The restrictions referred to in the previous point apply to both B2B and B2C relationships. Indeed, the Data Protection Law makes no distinction according to whether the recipient of the communication is a consumer or a business.

**9.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).**

The use of automated calling and communication systems, facsimile (fax) machines and electronic mail for the purposes of direct marketing may be allowed only in respect of Data Subjects who have given their prior consent. Moreover, there is no opt-out register to be checked in advance.

**9.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?**

To the best of our knowledge, there is no treaty or other agreement between Morocco and third countries in respect of international direct marketing. Thus, we are of the opinion that it is practically difficult for the CNDP to perform any enforcement against foreign entities in respect of marketing activities to Moroccan residents.

**9.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?**

Yes. The CNDP is increasingly strict and vigilant with regard to the Controller's use of Personal Data, particularly with regard to direct prospecting.

**9.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?**

The transfer of Personal Data by the Controller to third parties is possible if the Controller has clearly informed the Data Subject about the possibility of transferring its Personal Data and that the Data Subject has given its specific consent to transfer this data to third parties.

**9.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?**

The processing of Personal Data, with knowledge of the Data Subject's opposition of the processing, or where such processing is for the purpose of prospecting, in particular commercial prospecting is punished by imprisonment from three months to one year and/or a fine from MAD 20,000 (approx. USD 2,250) to MAD 200,000 (approx. USD 22,500).

## 10 Cookies

**10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).**

Morocco has not implemented specific legislation on cookies. However, as to the understanding of the CNDP, cookies do typically include Personal Data and therefore require a legal basis. Thus, pursuant to the CNDP's guidelines on the compliance of the websites dated April 2014, a website that uses cookies using Personal Data should obtain the prior consent of the Data Subject. In the same way, the website should specify the purpose of the use of cookies and explain to the Data Subject the means of opposing it.

**10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?**

As it stands, the applicable legislation does not expressly distinguish between different types of cookies.

**10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?**

We are not aware of whether the CNDP has ever taken any enforcement action in relation to cookies.

**10.4 What are the maximum penalties for breaches of applicable cookie restrictions?**

There are no specific sanctions applicable to the unlawfulness of the use of cookies. The CNDP would therefore, if the qualifications and legal conditions were met, enforce some sanctions related in particular to (i) the collection of data without the prior consent of the Data Subjects, (ii) the failure to comply with the purposes of the processing, and (iii) the failure to comply with the prior requirement to notify the CNDP.

## 11 Restrictions on International Data Transfers

**11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.**

A data transfer abroad can only take place under certain conditions and is subject to the prior CNDP's authorisation (please see the answers to questions 11.2 and 11.3).

**11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).**

The Controller duly declared or authorised by the CNDP to process Personal Data cannot transfer it to a foreign country except if this country provides a sufficient privacy protection level and that it respects fundamental rights of individual's data processing.

The acceptable privacy protection level that is given by a State is assessed in particular with: (i) the applicable data protection in force of this State; (ii) the security measures applied to such protection; (iii) the specific characteristics of data protection process including its object and duration; and (iv) the nature, origin and destination of the processed data.

The CNDP defines the list of foreign States meeting the above criteria. The current list includes: Austria; Belgium; Bulgaria; Canada; Cyprus; Czech Republic; Denmark; Estonia; Finland; France; Germany; Greece; Hungary; Iceland; Ireland; Italy; Latvia; Liechtenstein; Lithuania; Luxembourg; Malta; Netherlands; Norway; Poland; Portugal; Romania; Slovakia; Slovenia; Spain; Sweden; Switzerland; and the United Kingdom.

Besides, Controllers may transfer personal data to countries that do not offer adequate protection when:

1. the Data Subject gives their consent to the transfer of their Personal Data;
2. the transfer is necessary for: (i) the safeguard of the Data Subject's life; (ii) the protection of the public interest; (iii) complying with obligations allowing the acknowledgment, the exercise or the defence of a legal right; (iv) the enforcement of a contract between the Controller and the Data

Subject, or for pre-contractual measures undertaken at the individual's request; (v) the entry into or the performance of an agreed contract or for re-contract to be agreed upon; (vi) the performance of a contract, in the interest of the Data Subject, between the Controller and Third party; (vii) the performance of international mutual judicial assistance; or (viii) the prevention, diagnostic and treatment of medical treatment;

3. the transfer is made in application of a unilateral or multilateral agreement to which Morocco is a party; or
4. with a special explicit and motived decision of the CNDP when the process guarantees sufficient privacy protection along with the freedom and fundamental rights of person, especially on the ground of contractual clauses or internal rules to which it is subject.

**11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.**

Any transfer of Personal Data aboard should be approved by the CNDP in accordance with the following procedure:

1. Filling in the form relating to the transfer abroad of personal data (Form No. 118 available on the CNDP website).
2. Attaching the following documents to the Form:
   i. the Power of Attorney ("**PoA**") of the form signatory;
   ii. the document that proves the consent of the Data Subject, if any;
   iii. the references of the declaration receipt or authorisation certificate granted by the CNDP if any;
   iv. the Binding Corporate Rules if any;
   v. the processing authorisation delivered by the data protection authority of the recipient country if any; and
   vi. any other useful documents.
3. The above list of documents is not comprehensive and the authorisation procedure is organised on a case-by-case basis. Therefore, the CNDP can request or exclude any document from being necessary or not in considering the application.
4. The application is presented by the Controller or by the representative PoA.
5. The authorisation application is free of charge and is notified to the CNDP by (i) registered letter, (ii) hand delivering to the CNDP's secretariat, or (iii) electronic means against acknowledgment of receipt received by email.
6. The CNDP shall give its decision, within two months from the date of receipt of the authorisation's application. This time limit may be extended once. However, if the file is incomplete, the Controller is informed and the time limit starts when the requested information or document are provided.

It should be noted that when the CNDP has not taken a decision within the aforementioned period, i.e. four months, the authorisation is deemed to have been granted.

**11.4 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?**

This is not applicable.

**11.5 What guidance (if any) has/have the data protection authority(ies) issued in relation to the European Commission's revised Standard Contractual Clauses?**

This is not applicable.

## 12 Whistle-blower Hotlines

**12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?**

The CNDP has issued on May 31, 2013 the resolution No. 351-2013 relating to the conditions of implementation of whistleblower hotlines. The resolution provides that the whistle-blower hotlines should be limited to report the (i) breach of competition rules, (ii) conflicts of interest, (iii) insider trading, (iv) falsification of documents, accounts or audit reports, (v) theft or fraud, (vi) corruption, (vii) discrimination, and (viii) sexual harassment.

Moreover, the CNDP underline the following conditions to implement whistleblowing hotlines:

i. the use of the hotline should be optional;
ii. anonymous reporting must be discouraged (see the answer to question 12.2);
iii. the processing of the reports should be entrusted to a specific department or organisation subject to the confidentiality rules;
iv. the Controller should provide the Data Subjects with clear and complete information in respect of the whistle-blower hotline;
v. the respondent rights of information, opposition, access, rectification and deletion should be respected; and
vi. the CNDP should be notified prior to the implementation of the hotline.

**12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?**

Anonymous reporting is discouraged. Indeed, the CNDP is of the opinion that the identification of the report's author makes it possible to avoid the abusive use of the hotline and could improve the conditions of investigations by asking the whistle-blower additional questions.

## 13 CCTV

**13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?**

A CCTV system can only be implemented in workplaces and common private areas and is subject to prior declaration to the CNDP.

Pursuant to the CNDP's guidelines on CCTV, the cameras can be placed in any location that allows for the security of goods and/or persons but never in a place where there is a risk of infringement on the privacy of the latter. Thus, the cameras must not be used to monitor one or more employees, premises of worship and union, washrooms, meeting rooms or break areas, etc.

Moreover, the Controller is required to inform the Data Subjects by means of a high-visibility pictogram placed at the entrance to the supervised establishments.

**13.2 Are there limits on the purposes for which CCTV data may be used?**

The purpose of implementing a CCTV system should be limited to the safeguarding of goods and persons.

## 14 Employee Monitoring

**14.1 What types of employee monitoring are permitted (if any), and in what circumstances?**

There is no explicit governing of employee monitoring. The standards provided by the Data Protection Law should be expected to apply to any data processed as a result of operating such a monitoring. More specifically, the permissibility of employee monitoring has to be checked on a case-by-case basis and, as a general rule, full-time monitoring is not permitted.

Some types of monitoring are typically permissible, such as CCTV (please refer to section 13), geolocation of vehicles driven by employees, biometric access to the workplaces and temperature checking for the purposes of COVID-19. Such measures are subject, depending on the nature of the data collected, either with to prior authorisation of the CNDP or to a simple declaration to the CNDP.

The CNDP has yet to state its position with regard to phone and mailbox monitoring.

**14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.**

Employees subject to electronic monitoring should be informed in advance by their employer of the existence of such devices. In addition, employees must give their free and informed consent to the existence of these monitoring systems.

In practice, employees express their consent through a specific clause in their employment agreement regarding all types/purposes of data processing by the employer. The execution of a separate agreement for data processing is also permitted and is frequently used when the employment agreement already executed does not include a specific clause relating to the collection and processing of Personal Data.

**14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?**

Pursuant to article 466 of the Moroccan labour code of September 13, 2003, works councils must be informed of the structural and technological changes to be made to their workplaces.

More specifically, the Controller should inform the employee representative bodies, by mail, within a reasonable period of time, prior to the installation of the geolocation device in the companies' vehicles.

## 15 Data Security and Data Breach

**15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?**

Both Controllers and Processors should ensure they have appropriate technical and organisational measures to collect and process Personal Data in a way that guarantees security and safeguards against unauthorised or unlawful processing, accidental loss, destruction and damage of the data.

**15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

There is no legal requirement to report data breaches to the CNDP, and so far, there are no guidelines for voluntary breach reporting to the CNDP.

**15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

There is no legal requirement to report data breaches to the Data Subjects, and so far, there are no guidelines for voluntary breach reporting to the Data Subjects.

**15.4 What are the maximum penalties for data security breaches?**

According to the Data Protection Law, the penalties for data security breaches are up to one year of imprisonment and/or a fine of MAD 200,000 (approx. USD 22,500).

## 16 Enforcement and Sanctions

**16.1 Describe the enforcement powers of the data protection authority(ies).**

a. **Investigative Powers**: The CNDP is entitled to conduct visits of inspection *ex officio* at any company, in order to determine its compliance with the Data Protection Law. The CNDP's agents are indeed empowered to (i) access the data undergoing processing, (ii) require direct access to the premises in which the processing is undertaken, and (iii) collect and enter all the information and documents required to complete the investigative functions.

b. **Corrective Powers**: The Data Protection Law grants to the CNDP a wide range of powers including: the issuance of warnings or reprimands for non-compliance; ordering the blocking, erasure or destruction of Personal Data; imposing a permanent or temporary ban on processing; and withdrawing an authorisation and to impose an administrative fine.

c. **Authorisation and Advisory Powers**: The CNDP is the only data protection authority entrusted to grant the Controller the declaration receipt or authorisation certificate to collect and process data. The authority is also entitled to advise and give its opinion to the government or parliament about regulations in respect of data protection.
d. **Imposition of administrative fines for infringements of specified GDPR provisions**: This is not applicable.
e. **Non-compliance with a data protection authority**: The Controller who refuses to implement the decisions of the CNDP is subject to an imprisonment for three months to one year and/or a fine of MAD 10,000 (approx. USD 1,120) to MAD 100,000 (approx. USD 11,200).

**16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?**

The Data Protection Law entitles the CNDP to impose a temporary or definitive limitation, including a ban on processing.

**16.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.**

The CNDP approach in exercising its powers is both anticipative and reactive. Firstly, the anticipative approach is the result of a large publication of guidelines, reports, and advertising spots to offer advice and recommendations to the Controllers and Data Subjects. Secondly, the reactive approach involves decisions in respect of the Controllers infringements and recommendations to the government, parliament and public authorities regarding data protection matter.

**16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?**

There is no publicly available data on this matter.

## 17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

**17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?**

There is no publicly available data on this matter. We are of the opinion that any e-discovery requests or requests for disclosure from foreign law enforcement agencies have to be validated first by the Moroccan Courts in order for them to be validly enforced in Morocco.

**17.2 What guidance has/have the data protection authority(ies) issued?**

There are no guidelines with respect to e-discovery and disclosure to foreign law enforcement agencies.

## 18 Trends and Developments

**18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.**

There is no publicly available data on this matter.

**18.2 What "hot topics" are currently a focus for the data protection regulator?**

The COVID-19 pandemic has resulted in an explosion of digitalisation of businesses and a broad use of home offices. The CNDP have already issued resolutions on this, in particular in respect of (i) the telework in the sector of the customer relationship, and (ii) temperature checking for COVID-19 safety.

Furthermore, the CNDP ensures that the rights of the Data Subjects are respected within the framework of the vaccination campaign against COVID-19 and actually works on the conditions for bringing telemedicine into compliance with the Data Protection Law.

**Ayoub Berdai** is a lawyer holding a Master's degree in business law and a Ph.D. candidate. He joined Hajji & Associés in 2018 and has assisted domestic and international clients in corporate, data protection compliance, investment, commercial litigation, mergers and acquisitions, international financing and international arbitration. Ayoub Berdai is one of the three co-founders of the Mizan Arbiration Center in Casablanca.

**Hajji & Associés**
28 Bld. Moulay Youssef
Casablanca
Morocco

Tel: +212 522 48 74 74
Email: a.berdai@ahlo.ma
URL: www.ahlo.ma

Hajji & Associés is an independent Moroccan law firm which has developed, since the mid-1990s, high-level expertise in the international business law field.
The activities of the firm cover particular areas of international finance, the restructuring of companies, mergers and acquisitions, energy and infrastructure, market entry plans, IT law, commercial litigation and international arbitration.
The firm maintains privileged professional relationships with large international law firms, which generally support their clients' investment projects in Morocco with the assistance of Hajji & Associés.

**www.ahlo.ma**

# Norway


Gry Hvidsten

Emily M. Weitzenboeck

Wikborg Rein Advokatfirma AS


## 1 Relevant Legislation and Competent Authorities

### 1.1 What is the principal data protection legislation?

The principal data protection legislation in the EU is Regulation (EU) 2017/679 (the "General Data Protection Regulation" or "GDPR"). The GDPR repeals Directive 95/46/EC (the "Data Protection Directive") and has thereby led to increased (though not total) harmonisation of data protection law across the EU Member States. As Norway is not an EU Member State but part of the European Economic Area ("EEA"), the GDPR had to be incorporated into the EEA Agreement before it could be implemented into national law. The GDPR was incorporated into national law by means of the new Personal Data Act, which has been in effect since 20 July 2018.

### 1.2 Is there any other general legislation that impacts data protection?

The Electronic Communications Act of 25 July 2003 regulates the use of cookies on websites in section 2-7 b. This Act implements the requirements of Directive 2002/58/EC (as amended by Directive 2009/136/EC) (the "ePrivacy Directive").

In addition, the Marketing Control Act (Act of 9 January 2009 No. 2) regulates marketing communications (see question 9.1).

### 1.3 Is there any sector-specific legislation that impacts data protection?

Various pieces of sectorial legislation impact data protection, including the Personal Health Data Filing System Act (Act of 20 June 2014 No. 43) and the various regulations pertaining thereto. Furthermore, the Act on Patient Medical Records (Act of 20 June 2014 No. 42), the Health Research Act (Act of 20 June 2008 No. 44), the Therapeutic Biobanks Act (Act of 21 February 2003 No. 12), chapter 8 of the Health Personnel Act (Act of 2 July 1999 No. 64), chapter 5 of the Patient Rights Act (Act of 2 July 1999 No. 63), the Act on Police Records (Act of 28 May 2010 No. 16) and the Schengen Information Systems Act (Act of 16 July 1999 No. 66) and its regulations, also impact data protection.

These sector-specific laws were retained after the implementation of the GDPR but relevant provisions were amended to ensure compliance and coherence with the GDPR and the new Personal Data Act.

### 1.4 What authority(ies) are responsible for data protection?

The Norwegian Data Protection Authority (hereinafter referred to as "NDPA") oversees and enforces the Personal Data Act and the GDPR. It is an independent administrative body that reports annually to the *Storting* (Parliament). The current Data Protection Commissioner (*direktør*) is Bjørn Erik Thon, who was appointed in August 2010 and whose appointment was renewed for another six-year term from August 2016.

Data controllers within the health sector are additionally regulated by the various pieces of health sector legislation relating to the processing of medical health data.

The Norwegian Communications Authority ("Nkom") oversees and enforces the Electronic Communications Act, including compliance with the cookie provisions.

## 2 Definitions

### 2.1 Please provide the key definitions used in the relevant legislation:

- "**Personal Data**"
  "Personal Data" means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- "**Processing**"
  "Processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- "**Controller**"
  "Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- "**Processor**"
  Processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

- "**Data Subject**"
  "Data Subject" means an individual who is the subject of the relevant personal data.
- "**Sensitive Personal Data**"
  The term used in the Personal Data Act, like the GDPR, is "special categories of personal data"; these are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health or sex life and sexual orientation, genetic data or biometric data.
- "**Data Breach**"
  "Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
- **Other key definitions – please specify (e.g., "Pseudonymous Data", "Direct Personal Data", "Indirect Personal Data")**
  The Personal Health Data Filing System Act of 2014 refers to "characteristics that directly identify a natural person" (*direkte personidentifiserende kjennetegn*). The term is, however, not defined and must be understood in light of the meaning of "personal data" in the GDPR and the new Personal Data Act; see also the term "indirectly identifiable health data" below. Likewise, some sector-specific health legislation, such as the Health Personnel Act, refers to "characteristics that directly identify a natural person" (*direkte personentydige kjennetegn*). The term is also to be interpreted in light of "personal data".
  The Personal Health Data Filing System Act of 2014 refers to the term "indirectly identifiable health data" (*indirekte identifiserbare helseopplysninger*) as "health data in which the name, national identity number and other characteristics that identify a person [*personentydige kjennetegn*] are removed, but where the data may nevertheless be linked to an individual".

## 3 Territorial Scope

### 3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The Personal Data Act applies to the processing of personal data that is carried out in connection with the activities of an establishment of a controller or processor in Norway, and regardless of whether or not the processing takes place in the EEA or not.

A business that is not established in Norway but is subject to the laws of Norway by virtue of public international law is also subject to the Personal Data Act.

The Personal Data Act applies to businesses outside the EEA if they (either as controller or processor) process personal data of Norwegian residents in relation to: (i) the offering of goods or services (whether or not in return for payment) to Norwegian residents; or (ii) the monitoring of the behaviour of Norwegian residents (to the extent that such behaviour takes place in Norway).

## 4 Key Principles

### 4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  Personal data must be processed lawfully, fairly and in a transparent manner. Controllers must provide certain minimum information to data subjects regarding the collection and further processing of their personal data. Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
- **Lawful basis for processing**
  Processing of personal data is lawful only if, and to the extent that, it is permitted under EU data protection law. The GDPR provides an exhaustive list of legal bases on which personal data may be processed, of which the following are the most relevant for businesses: (i) prior, freely given, specific, informed and unambiguous consent of the data subject; (ii) contractual necessity (i.e., the processing is necessary for the performance of a contract to which the data subject is a party, or for the purposes of pre-contractual measures taken at the data subject's request); (iii) compliance with legal obligations (i.e., the controller has a legal obligation, under the laws of the EU or an EU Member State, to perform the relevant processing); or (iv) legitimate interests (i.e., the processing is necessary for the purposes of legitimate interests pursued by the controller, except where the controller's interests are overridden by the interests, fundamental rights or freedoms of the affected data subjects).
  Please note that businesses require stronger grounds to process sensitive personal data. The processing of sensitive personal data is only permitted under certain conditions, of which the most relevant for businesses are: (i) explicit consent of the affected data subject; (ii) the processing is necessary in the context of employment law; or (iii) the processing is necessary for the establishment, exercise or defence of legal claims.
- **Purpose limitation**
  Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes. If a controller wishes to use the relevant personal data in a manner that is incompatible with the purposes for which they were initially collected, it must be able to rely on the data subject's consent as a legal basis or the further processing must be permitted by law.
- **Data minimisation**
  Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed. A business should only process the personal data that it actually needs to process in order to achieve its processing purposes.
- **Proportionality**
  The cumulative requirements of the principle of proportionality are fulfilled by compliance with the requirements of other basic principles.
- **Retention**
  Personal data must be kept in a form that permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of the GDPR, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of the data subject.
- **Accuracy**
  Personal data must be accurate and, where necessary, kept up to date. A business must take every reasonable step to ensure that personal data that are inaccurate are either erased or rectified without delay.

- **Data security**
  Personal data must be processed in a manner that ensures appropriate security of those data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- **Accountability**
  The controller is responsible for, and must be able to demonstrate, compliance with the data protection principles set out above.

## 5 Individual Rights

### 5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**
  A data subject has the right to obtain from a controller the following information in respect of the data subject's personal data: (i) confirmation of whether, and where, the controller is processing the data subject's personal data; (ii) information about the purposes of the processing; (iii) information about the categories of data being processed; (iv) information about the categories of recipients with whom the data may be shared; (v) information about the period for which the data will be stored (or the criteria used to determine that period); (vi) information about the existence of the rights to erasure, to rectification, to restriction of processing and to object to processing; (vii) information about the existence of the right to complain to the relevant data protection authority; (viii) where the data were not collected from the data subject, information as to the source of the data; and (ix) information about the existence of, and an explanation of the logic involved in, any automated processing that has a significant effect on the data subject.
  Additionally, the data subject may request a copy of the personal data being processed.
- **Right to rectification of errors**
  Controllers must ensure that inaccurate or incomplete data are erased or rectified. Data subjects have the right to rectification of inaccurate personal data.
- **Right to deletion/right to be forgotten**
  Data subjects have the right to erasure of their personal data (the "right to be forgotten") if: (i) the data are no longer needed for their original purpose (and no other lawful purpose exists); (ii) the lawful basis for the processing is the data subject's consent, the data subject withdraws that consent, and no other lawful ground exists; (iii) the data subject exercises the right to object, and the controller has no overriding grounds for continuing the processing; (iv) the data have been processed unlawfully; or (v) erasure is necessary for compliance with EU law or national data protection law.
- **Right to object to processing**
  Data subjects have the right to object, on grounds relating to their particular situation, to the processing of personal data where the basis for that processing is either the performance of a task carried out in the public interest or in the exercise of official authority, or where the basis for the processing is the legitimate interest of the controller. The controller must cease such processing unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the relevant data subject, or requires the data in order to establish, exercise or defend legal rights.
  The data subject also has a right to object to processing for direct marketing purposes; see below.
- **Right to restrict processing**
  Data subjects have the right to restrict the processing of personal data, which means that the data may only be held by the controller, and may only be used for limited purposes if: (i) the accuracy of the data is contested by the data subject (and only for as long as it takes to verify that accuracy); (ii) the processing is unlawful and the data subject requests restriction (as opposed to exercising the right to erasure); (iii) the controller no longer needs the data for their original purpose, but the data are still required by the data subject to establish, exercise or defend legal claims; or (iv) verification of overriding grounds is pending, in the context of the data subject's exercise of his/her right to object to processing.
- **Right to data portability**
  Data subjects have a right to receive a copy of their personal data in a commonly used machine-readable format, and to transmit their personal data from one controller to another or have the data transmitted directly between controllers. This right applies where the basis for the processing is the data subject's consent or where the processing is necessary for the performance of a contract with the data subject.
- **Right to withdraw consent**
  A data subject has the right to withdraw his/her consent at any time. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject must be informed of the right to withdraw consent. It must be as easy to withdraw consent as to give it.
- **Right to object to marketing**
  Data subjects have the right to object to the processing of personal data for the purpose of direct marketing, including profiling.
- **Right to complain to the relevant data protection authority(ies)**
  Data subjects have the right to lodge complaints concerning the processing of their personal data with the NDPA, if the data subjects live or work in Norway or the alleged infringement occurred in Norway.
- **Other key rights – please specify**
  The data subject has the right not to be subject to a fully automated decision, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her, except if the decision: (i) is necessary for the entering into, or performance of, a contract with the data subject; (ii) is authorised by EU or national law to which the controller is subject and which lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interest; or (iii) is based on the data subject's explicit consent. Where the decision is carried out on the grounds specified in (i) or (iii) as aforementioned, the data subject has the right to obtain human intervention by the controller, to express his or her view and to contest the decision.
  Automated decisions may not be based on sensitive personal data unless the processing is based on either the data subject's consent or is for reasons of substantial public interest based on EU or national law and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

## 6 Registration Formalities and Prior Approval

**6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?**

There is no legal obligation on businesses to register with or notify the NDPA in respect of their processing activities. Note, however, that there are some transitional provisions related to prior approval/licences given prior to the implementation of the GDPR in Norway; most notably licences to perform credit reporting, licences to carry out integrity due diligence, and licences to perform doping controls at certain fitness establishments.

Please also note that, in some instances, businesses are obliged to consult with the NDPA before the processing starts. This especially pertains to certain high-risk processing. The government has the power to implement specific regulations regarding prior consultation and prior authorisation, but so far, no such regulations have been enacted.

**6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?**

This is not applicable.

**6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?**

This is not applicable.

**6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?**

This is not applicable.

**6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?**

This is not applicable.

**6.6 What are the sanctions for failure to register/notify where required?**

This is not applicable.

**6.7 What is the fee per registration/notification (if applicable)?**

This is not applicable.

**6.8 How frequently must registrations/notifications be renewed (if applicable)?**

This is not applicable.

**6.9 Is any prior approval required from the data protection regulator?**

No prior approval from the data protection regulator is required. However, according to the new Personal Data Act, in exceptional circumstances, the NDPA may permit the processing of special categories of personal data where the processing is necessary for important public interests. In such cases, the NDPA shall lay down conditions to protect the data subject's fundamental rights and interests. The government has the power to adopt regulations to allow the processing of special categories of personal data where this is necessary for important public interests. Such regulations shall lay down appropriate and special measures to protect the data subject's fundamental rights and interests.

**6.10 Can the registration/notification be completed online?**

This is not applicable.

**6.11 Is there a publicly available list of completed registrations/notifications?**

This is not applicable.

**6.12 How long does a typical registration/notification process take?**

This is not applicable.

## 7 Appointment of a Data Protection Officer

**7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.**

The appointment of a Data Protection Officer for controllers or processors is mandatory in some circumstances, including where the core activity of the data controller consists of: (i) large-scale regular and systematic monitoring of individuals; or (ii) large-scale processing of special categories of personal data. The appointment of a Data Protection Officer is also mandatory where processing is carried out by a public authority or body. In the preparatory works to the Personal Data Act, the Justice Department specifies that this comprises the administrative bodies that fall within section 2, first paragraph, letter "a" of the Public Administration Act, i.e., any state, county authority or municipal body.

Where a business designates a Data Protection Officer voluntarily, the requirements of the GDPR apply as though the appointment was mandatory.

**7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?**

In the circumstances where the appointment of a Data Protection Officer is mandatory, failure to comply may result in a wide range of penalties available under the GDPR.

**7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?**

The appointed Data Protection Officer should not be dismissed or penalised for performing their tasks and should report directly to the highest management level of the controller or processor.

**7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?**

A single Data Protection Officer is permitted by a group of undertakings provided that the Data Protection Officer is easily accessible from each establishment.

**7.5 Please describe any specific qualifications for the Data Protection Officer required by law.**

The Data Protection Officer should be appointed on the basis of professional qualities and should have expert knowledge of data protection law and practices. While this is not strictly defined, it is clear that the level of expertise required will depend on the circumstances. For example, the involvement of large volumes of sensitive personal data will require a higher level of knowledge.

**7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?**

A Data Protection Officer should be involved in all issues which relate to the protection of personal data. The GDPR outlines the minimum tasks required by the Data Protection Officer, which include: (i) informing the controller, processor and their relevant employees who process data of their obligations under the GDPR; (ii) monitoring compliance with the GDPR, national data protection legislation and internal policies in relation to the processing of personal data including internal audits; (iii) advising on data protection impact assessments ("DPIA") and the training of staff; and (iv) cooperating with the relevant data protection authority and acting as the authority's primary contact point for issues related to data processing.

**7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?**

Yes, the controller or processor must communicate the contact details of the Data Protection Officer to the NDPA. The NDPA has set up a registration system where organisations can register the contact details of the Data Protection Officer. Registration may be made online.

**7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?**

The Data Protection Officer does not necessarily need to be named in the public-facing privacy notice. However, the contact details of the Data Protection Officer must be notified to the data subject when personal data relating to that data subject are collected. Furthermore, the GDPR requires that the contact details of the Data Protection Officer be published. As a matter of good practice, it is recommended in guidelines issued by the Article 29 Working Party ("WP29") (and endorsed by the European Data Protection Board, henceforth "EDPB") that an organisation informs its employees of the name and contact details of the Data Protection Officer. The guidelines also state that the communication of the name of the Data Protection Authority to the supervisory authority is essential in order for the Data Protection Officer to serve as a contact point between the organisation and the supervisory authority.

## 8 Appointment of Processors

**8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?**

Yes. The business that appoints a processor to process personal data on its behalf is required to enter into an agreement with the processor which sets out the subject matter for processing, the duration of processing, the nature and purpose of processing and the obligations and rights of the controller (i.e., the business) and of the processor. See further question 8.2.

It is essential that the processor appointed by the business complies with the GDPR.

**8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?**

The processor must be appointed under a binding agreement in writing. The contractual terms must stipulate that the processor: (i) only acts on the documented instructions of the controller; (ii) imposes confidentiality obligations on all employees and others authorised to process personal data; (iii) ensures the security of personal data that it processes; (iv) abides by the rules regarding the appointment of sub-processors; (v) implements measures to assist the controller with guaranteeing the rights of data subjects; (vi) assists the controller in ensuring compliance with the controller's obligations to ensure the security of personal data, the notification of a personal data breach, the carrying out of a DPIA and prior consultation; (vii) either returns or destroys the personal data at the end of the relationship (except as required by EU or Member State law); and (viii) provides the controller with all information necessary to demonstrate compliance with the GDPR.

## 9 Marketing

**9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).**

Marketing communications may not be directed at natural persons during the course of trade (using electronic methods of communication which permit individual communication, such as electronic mail, telefax or automated calling systems) without the prior consent of the recipient. Such prior consent shall not, however, apply to marketing:

(a) where the natural person is contacted orally by telephone; or

(b) by means of electronic mail where there is an existing customer relationship and the contracting trader has obtained the electronic address of the customer in connection with a sale. The marketing may only relate to the trader's own goods, services or other products corresponding to those on which the customer relationship is based. At the time that the electronic address is obtained, and at the time of any subsequent marketing communication, the customer shall be given a simple and free opportunity to opt out of receiving such communications.

**9.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?**

The restrictions specified in the answer to question 9.1 apply to electronic direct marketing to all natural persons. Marketing communications sent to a person's private email address, mobile phone ("SMS") or fax machine are included in the prohibition. Furthermore, marketing communications sent to a natural person's individual email address at work, irrespective of whether the email includes offers to the organisation or not, are also included in the prohibition.

**9.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).**

According to the Marketing Control Act, consumers may opt out of marketing by telephone or by addressed post by registering in the Central Marketing Exclusion Register. Consumers and natural persons may also opt out by contacting the trader directly.

With regard to telephone marketing, businesses cannot contact consumers who have opted out of marketing by registering in the Central Marketing Exclusion Register or contact natural persons who have opted out of such marketing directly with the trader unless: (i) the natural person has made an express request to a specific trader concerning receiving such marketing from the trader (such request may be withdrawn at any time); or (ii) in the case where consumers have opted out of marketing in the Central Marketing Exclusion Register, there is an existing customer or donor relationship and the trader has received the consumer's contact information in connection with sales or fundraising. Such marketing can only relate to the trader's own products that correspond to those on which the customer or donor relationship is based.

The same prohibitions and restrictions as those described in the preceding paragraph apply with regard to direct marketing by addressed post.

Telephone marketing to consumers on Saturdays, Sundays, public holidays or on weekdays before 09:00 or after 21:00 is prohibited. It is also prohibited to direct telephone marketing to consumers from a hidden telephone number or from a telephone number that is not registered and cannot be found in telephone directories.

The Central Marketing Exclusion Register shall enable consumers, if they so wish, to opt out of marketing from anyone other than voluntary organisations. Traders are obliged to update their address register in line with the Central Marketing Exclusion Register before their first inquiry, and before inquiry in the month when the marketing is conducted. Traders must also make sure that natural persons, easily and without cost, can opt out of marketing directly with the trader.

**9.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?**

Yes, the Marketing Control Act applies to all actions and terms aimed at consumers or businesses in Norway.

**9.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?**

No, compliance with the provisions of the Marketing Control Act, mentioned in questions 9.1 to 9.4 above, is monitored by the Consumer Authority (formerly known as the Consumer Ombudsman) and the Market Council.

**9.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?**

A marketing list from third parties may be used for telephone marketing and/or marketing by addressed post provided that the conditions, restrictions and prohibitions specified in questions 9.1 and 9.2 are adhered to.

As regards electronic direct marketing, in practice, marketing lists from third parties rarely satisfy the legal requirements for use for marketing via electronic methods of communication which permit individual communication (e.g., email, SMS) pursuant to section 15 of the Marketing Control Act. A marketing list from third parties cannot be used for marketing via electronic methods of communication which permit individual communication, unless the prior consent of the recipient (customer) for such type of direct marketing has been obtained beforehand. Such consent must be specific, informed, freely given and unambiguous. According to guidelines from the Consumer Authority, the requirement for informed consent means that, when consent is being collected, the consumer must have been informed about who the consent is being given to. If the consent is collected on behalf of an organisation's business partners, this must be clearly indicated and there must be an updated list of names of all such business partners in the consent declaration, together with a description of the type of marketing that these will be sending and the extent thereof. Furthermore, such prior consent cannot be collected via electronic methods of communications such as email; i.e., a business cannot communicate via email or SMS with a consumer to ask whether he/she wishes to consent to marketing via email, SMS or other electronic method of communication falling within section 15 of the Marketing Control Act.

**9.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?**

The Consumer Council and the Market Council may impose an enforcement penalty (*tvangsmulkt*) or an infringement penalty (*overtredelsesgebyr*). When determining the amount of an enforcement penalty, which could take the form of a running charge or a lump sum, emphasis is given to the consideration that it must not be profitable to breach the decision of the Council or Market Council. In the determination of the amount of an infringement penalty, emphasis is given to the severity, scope and effects of the infringement.

## 10 Cookies

**10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).**

The Electronic Communications Act of 25 July 2003, as amended with effect from 1 July 2013, regulates the use of cookies on websites in section 2-7 b. This Act implements the requirements of Article 5 of Directive 2002/58/EC (as amended by Directive 2009/136/EC) (the "ePrivacy Directive") in relation to the use of cookies.

According to section 2-7 b of the Electronic Communications Act, the storage of data in the user's communications equipment, or access thereto, is not permitted unless the user is informed of what data are processed, the purpose of the processing, who is processing the data; and unless the user has consented thereto. The aforesaid does not hinder technical storage of or access to data: (a) exclusively for the purpose of transmitting a communication in an electronic communications network; or (b) where the cookie is strictly necessary to provide an "information society service" (e.g., a service over the internet) requested by the subscriber or user, which means that it must be essential to fulfil their request.

The consent of the end user is a prerequisite for cookies to be used. The user must have the possibility to withdraw his/her consent. Following the judgment by the European Court of Justice in case C-673/17 (Planet49), the prevailing opinion is that the requirement for consent to cookies must be interpreted in line with the consent requirements in the GDPR).

**10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?**

No, they do not.

**10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?**

In 2015, Nkom initiated a review of Norwegian websites to determine how such websites are implementing the requirements of the aforementioned section 2-7 b. Nkom looked at the 500 most visited Norwegian websites. Four out of five of the investigated websites were found to be non-compliant. Nkom contacted the non-compliant websites and stated that it would re-examine the websites to verify compliance. No infringement penalties have been issued so far.

If there is refusal to abide by the information requirements, the sanction mechanisms in the law consist of the issue of an order to rectify one's position and/or an infringement penalty.

**10.4 What are the maximum penalties for breaches of applicable cookie restrictions?**

Breach of section 2-7 b may give rise to an infringement penalty (*overtredelsesgebyr*); its extent depends on the seriousness and length of the infringement, the degree of fault and the turnover of the business. According to the Electronic Communications Regulations, in the case of wilful or negligent infringement, the amount may be up to 5% of the turnover, with turnover being the total sales revenue of the business for the last accounting year; where the infringer is a group of companies and the infringement concerns the group members' activities, the turnover is the total sales revenue for the member firms that are active in the market affected by the infringement. Physical persons who wilfully or negligently infringe such provisions may incur an infringement penalty of up to 30 times the court fee (which at present is NOK 1,199); i.e., up to NOK 35,970.

According to section 12-4 of the Electronic Communications Act, wilful or negligent infringement may also give rise to criminal penalties punishable by the imposition of a fine or imprisonment for up to six months.

Where cookies are used for the processing of personal data in breach of the Personal Data Act, the sanction provisions in the Personal Data Act and the GDPR (see question 16.1) are applicable.

## 11 Restrictions on International Data Transfers

**11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.**

Data transfers to other jurisdictions that are not within the EEA can only take place if the transfer is to an "Adequate Jurisdiction" (as specified by the EU Commission) or the business has implemented one of the required safeguards as specified by the GDPR.

**11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).**

When transferring personal data to a country other than an Adequate Jurisdiction, businesses must ensure that there are appropriate safeguards on the data transfer as prescribed by the GDPR. The GDPR offers a number of ways to ensure compliance for international data transfers such as the use of Standard Contractual Clauses or Binding Corporate Rules ("BCRs").

Businesses can adopt the Standard Contractual Clauses drafted by the EU Commission – these are available for transfers between controllers, and transfers between a controller (as exporter) and a processor (as importer). When such Standard Contractual Clauses are used, no prior authorisation is required. International data transfers may also take place on the basis of contracts agreed between the data exporter and data importer, provided that they conform to the protections outlined in the GDPR and they have prior approval by the relevant data protection authority.

International data transfers within a group of businesses can be safeguarded by the implementation of BCRs. The BCRs will always need approval from the relevant data protection authority. Most importantly, the BCRs will need to include a mechanism to ensure they are legally binding and enforced by every member in the group of businesses. Among other things, the BCRs must set out the group structure of the businesses, the proposed data transfers and their purpose, the rights of data subjects, the mechanisms that will be implemented to ensure compliance with the GDPR, and the relevant complaint procedures.

**11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.**

Unless the controller or processor has already established a

GDPR-compliant mechanism for such transfers, as set out in question 11.2, or the transfer fails to adhere to the conditions set out in Article 49 of the GDPR which allow for derogations in specific situations, it is likely that an international data transfer will require prior approval from the data protection authority.

In any case, some of the safeguards outlined in the GDPR, such as the establishment of BCRs, will need initial approval from the relevant data protection authority.

**11.4 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?**

The NDPA has published a set of Questions-and-Answers (https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2020/sos-om-nye-regler-for-overforing/) on the new rules for transfer of personal data to countries that are outside the European Economic Area. The Q&A is in line with, and cross-refers to: (i) the EDPB's Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data; and (ii) the EDPB's Recommendations 01/2020 and 02/2020 on the European Essential Guarantees for surveillance measures.

**11.5 What guidance (if any) has/have the data protection authority(ies) issued in relation to the European Commission's revised Standard Contractual Clauses?**

The NDPA has published information on the new Standard Contractual Clauses (https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2021/nye-standardavtaler/). The new SCCs will have formal legal effect in Norway after they have been incorporated into the EEA Agreement.

## 12 Whistle-blower Hotlines

**12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?**

Internal whistle-blowing schemes are generally established in pursuance of a concern to implement proper corporate governance principles in the daily functioning of businesses. Whistle-blowing is designed as an additional mechanism for employees to report misconduct internally through a specific channel, and supplements a business' regular information and reporting channels, such as employee representatives, line management, quality-control personnel or internal auditors who are employed precisely to report such misconduct.

According to section 2 A-1 of the Working Environment Act, an employee has a right to notify censurable conditions at the employer's undertaking. The rules on notification of censurable conditions also apply with respect to the following persons when performing work in undertakings subject to the Working Environment Act: students at teaching or research institutions; national servicemen; persons performing civilian national service and civil defence servicemen; inmates in correctional institutions; patients in health or rehabilitation institutions and the like; trainees; and persons who, without being employees, participate in labour market schemes. Furthermore, workers hired from temporary-work agencies also have a right to notify censurable conditions at the hirer's undertaking. The term "censurable conditions" means conditions which are in breach of legal rules, written ethical guidelines in the undertaking or ethical norms to which there is broad adherence in society; for example, conditions that can involve: (a) danger to life or health; (b) danger to the climate or environment; (c) corruption or other economic crime; (d) misuse of authority; (e) an inexcusable working environment; or (f) a personal data breach.

According to section 2 A-6, an undertaking that regularly employs at least five employees must have procedures for internal notification. An undertaking with fewer than five employees must also have such procedures if the conditions at the undertaking so indicate. Procedures for internal notification in connection with systematic health, environment and safety work, must be prepared in cooperation with the employees and their representatives. The procedures shall not limit an employee's right to make a notification.

Procedures shall be in writing and must, as a minimum, contain: (a) an encouragement to notify censurable conditions; (b) the procedure for notification; and (c) the procedure for receipt, processing and follow-up of notifications. The procedures must be easily accessible to all employees at the undertaking.

**12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?**

Anonymous reporting is not prohibited under EU data protection law; however, it raises problems as regards the essential requirement that personal data should only be collected fairly. As a rule, WP29 considers that only identified reports should be communicated through whistle-blowing schemes in order to satisfy this requirement. WP29 holds that whistle-blowing schemes should be built in such a way that they do not encourage anonymous reporting as the usual way to make a complaint.

As regards Norway, according to the preparatory works to chapter 2 A (regarding whistle-blowing) of the Working Environment Act, the rules on notifying censurable conditions at the employer's undertaking do not prohibit anonymous whistle-blowing.

## 13 CCTV

**13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?**

A DPIA must be undertaken with assistance from the Data Protection Officer when there is systematic monitoring of a publicly accessible area on a large scale. If the DPIA suggests that the processing would result in a high risk to the rights and freedoms of individuals in the absence of measures taken to mitigate the risk, the controller must consult the data protection authority pursuant to Article 36 of the GDPR.

During the course of a consultation, the controller must provide information on the responsibilities of the controller and/or processors involved, the purpose of the intended processing, a copy of the DPIA, the safeguards provided by the GDPR to protect the rights and freedoms of data subjects and, where applicable, the contact details of the Data Protection Officer.

If the data protection authority is of the opinion that the CCTV monitoring would infringe the GDPR, it must provide written advice to the controller within eight weeks of the request of a consultation and can use any of its wider investigative, advisory and corrective powers outlined in the GDPR.

The Personal Data Act has a provision regarding the use of fake camera surveillance. According to section 31, when camera surveillance is in breach of the GDPR or the Personal Data Act, it is also not permitted to use fake camera surveillance equipment or, by a sign, placard or similar, give the impression that there is camera surveillance. The term "camera surveillance" in section 31 is defined in the second paragraph as meaning continuous or regularly repeated surveillance of persons by means of a remote-controlled or automatically operated video camera or similar device, which is permanently fixed. "Fake camera surveillance" is defined as equipment which can easily be confused with real camera surveillance.

With regard to camera surveillance of employees, see section 14 hereunder.

### 13.2 Are there limits on the purposes for which CCTV data may be used?

The GDPR does not have any specific provisions on CCTV. Thus, processing of personal data that occurs via CCTV is regulated by the GDPR's general rules in Article 6. How the GDPR's general rules will be applied with regard to the processing of personal data via CCTV, e.g., what constitutes the possibility of monitoring, deletion deadlines, notices, etc., will depend on further interpretation of the GDPR (see, e.g., Guidelines 3/2019 issued by the EDPB).

In the preparatory works to the Personal Data Act, the Ministry of Justice stated that it is not, at present, necessary to have provisions in national law which specifically make an exception from the prohibition in Article 9(1) for CCTV monitoring which has the purpose of capturing sensitive personal data.

With regard to camera surveillance of employees, see section 14 hereunder.

## 14 Employee Monitoring

### 14.1 What types of employee monitoring are permitted (if any), and in what circumstances?

Specific provisions regarding employee monitoring, pursuant to GDPR Article 88, have been implemented as regulations to the Working Environment Act.

One set of such regulations to the Working Environment Act contains provisions regarding video surveillance in places of the employer's undertaking that are frequented by a limited group of persons. Such video surveillance is subject to the general terms pursuant to the Working Environment Act chapter 9 on control measures in relation to employees, and is furthermore only permitted if, according to the activity, there is a need to prevent hazardous situations from arising and to protect the safety of employees or others, or if the surveillance is deemed essential for other reasons.

Another set of regulations to the Working Environment Act relate to the examination of employee emails and other electronically stored material. According to the regulations, an employer may only access email in an employee's email account (a) when necessary to maintain daily operations or other justified interests of the business, or (b) in cases of justified suspicion that the employee's use of email constitutes a serious breach of the duties that follow from the employment, or may constitute grounds for termination or dismissal. The aforementioned term "necessary" is interpreted restrictively. These provisions also apply to other personal workspaces in the undertaking's communication network, and other electronic equipment provided by the employer.

### 14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

According to the regulations regarding video surveillance in the employer's undertaking, attention must be drawn clearly, by means of a sign or in some other way, to the fact that a particular place is under surveillance, that the surveillance may include sound recordings, and to the identity of the controller.

According to the regulations regarding examination of employee emails and other electronically stored material, the employee shall be notified whenever possible and given an opportunity to speak before the employer makes any such examination. In the notice, the employer shall explain why the criteria mentioned above in question 14.1 are believed to have been met, and shall advise on the employee's rights. The employee shall, whenever possible, have the opportunity to be present during the examination, and has the right to the assistance of an elected employee representative or other representative. If the examination is made without prior warning, the employee shall receive subsequent written notification of the examination as soon as it is done.

### 14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

The general provisions in the Working Environment Act regarding control measures in relation to employees apply. Thus, an employer is, *inter alia*, obliged to discuss as early as possible the needs, designs, implementation and major changes to control measures in the undertaking with the employees' elected representatives.

See also question 14.2 above.

## 15 Data Security and Data Breach

### 15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Yes. Personal data must be processed in a way that ensures security and safeguards against unauthorised or unlawful processing, accidental loss, destruction and damage of the data.

Both controllers and processors must ensure they have appropriate technical and organisational measures to meet the requirements of the GDPR. Depending on the security risk, this may include the encryption of personal data, the ability to ensure the ongoing confidentiality, integrity and resilience of processing systems, the ability to restore access to data following a technical or physical incident, and a process for regularly testing and evaluating the technical and organisational measures for ensuring the security of processing.

**15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

The controller is responsible for reporting a personal data breach without undue delay (and in any case within 72 hours of first becoming aware of the breach) to the relevant data protection authority, unless the breach is unlikely to result in a risk to the rights and freedoms of the data subject(s). A processor must notify any data breach to the controller without undue delay.

The notification must include the nature of the personal data breach, including the categories and number of data subjects concerned, the name and contact details of the Data Protection Officer or relevant point of contact, the likely consequences of the breach, and the measures taken to address the breach, including attempts to mitigate possible adverse effects.

**15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

Controllers have a legal requirement to communicate the breach to the data subject, without undue delay, if the breach is likely to result in a high risk to the rights and freedoms of the data subject.

The notification must include the name and contact details of the Data Protection Officer (or point of contact), the likely consequences of the breach, and any measures taken to remedy or mitigate the breach.

The controller may be exempt from notifying the data subject if: the controller has implemented appropriate technical and organisational measures that render the personal data unintelligible (e.g., because the affected data is encrypted); the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise; or the notification requires a disproportionate effort, in which case there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

Pursuant to section 16 of the Personal Data Act, the duty to notify the data subject does not apply to the extent such notification will reveal information: (i) that is of importance to Norway's foreign political interests or national defence and security interests, when the controller can exempt such information pursuant to section 20 or section 21 of the Freedom of Information Act; (ii) that it is essential to keep secret for the purposes of preventing, investigating, revealing and judicial proceedings of criminal offences; and (iii) that, in statute or based on statute, is subject to confidentiality.

**15.4 What are the maximum penalties for data security breaches?**

The maximum penalty for breach of sections 32 to 34 of the GDPR is €10 million or 2% of worldwide turnover, whichever is higher; *cf.* GDPR Article 83(4)(a). In the case of a breach of Article 83(5), for example, breach of the principle of integrity and confidentiality as per Article 5(1)(f), the maximum penalty is €20 million or 4% of worldwide turnover, whichever is higher.

## 16 Enforcement and Sanctions

**16.1 Describe the enforcement powers of the data protection authority(ies).**

(a) **Investigative Powers**: The NDPA has wide powers to order the controller and the processor to provide any information it requires for the performance of its tasks, to conduct investigations in the form of data protection audits, to carry out reviews on certifications issued pursuant to the GDPR, to notify the controller or processor of alleged infringement of the GDPR, to obtain access from controllers and processors to all personal data and all information necessary for the performance of its tasks, and to access the premises of the data controller and processor, including any data processing equipment.

(b) **Corrective Powers**: The NDPA has a wide range of powers, including to issue warnings or reprimands for non-compliance, to order the controller to disclose a personal data breach to the data subject, to impose a permanent or temporary ban on processing, to withdraw a certification and to impose an administrative fine (as below).

(c) **Authorisation and Advisory Powers**: The NDPA has a wide range of powers to advise the controller, accredit certification bodies, issue certifications, authorise contractual clauses and administrative arrangements and approve binding corporate rules as outlined in the GDPR.

(d) **Imposition of administrative fines for infringements of specified GDPR provisions**: The GDPR provides for administrative fines which can be up to €20 million or up to 4% of the business' worldwide annual turnover from the preceding financial year, whichever is higher.

(e) **Non-compliance with a data protection authority**: The GDPR provides for administrative fines of €20 million or up to 4% of the business' worldwide annual turnover from the preceding financial year, whichever is higher. Furthermore, according to the Personal Data Act, the NDPA can impose a daily coercive fine which runs for each day following the expiry of the time limit set for compliance with the NDPA's order until the order has been complied with.

**16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?**

The GDPR entitles the relevant data protection authority to impose a temporary or definitive limitation, including a ban on processing.

**16.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.**

There are various examples that illustrate how the NDPA exercises its investigative and corrective powers.

In January 2021, the NDPA gave advance notice to the US company Grindr LLC of its intent to impose an administrative fine of NOK 100 million (*circa* €10 million) for having disclosed personal data, including sensitive personal data, to third party advertisers without a legal basis pursuant to articles 6 and 9 of the GDPR. This is the highest administrative fine in respect of which advance notice has been given by the NDPA and, if confirmed, would result in the highest NDPA fine to date.

Another example is the administrative fine of NOK 3 million (*circa* €276,000) imposed on Bergen Municipality in the autumn of 2020 for breaches of personal data security by the municipality's schools due to poor routines for processing home addresses where confidentiality was necessary. The municipality had not established nor communicated the necessary guidelines to secure the personal data of children and parents who had a confidential address before a new communication tool was put to use. Personal data that should have been confidential were thus available to unauthorised persons. The NDPA subsequently also sent a letter with guidance to the municipality's data processor where it pointed out the data processor's duty to ensure compliance with its data processing agreement with the municipality.

**16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?**

The GDPR can also apply to non-EEA businesses even if they have no physical presence in the EEA (see the answer to question 3.1 above). Such businesses must appoint a representative in the EEA against which the NDPA or the relevant data protection authority can take relevant enforcement action under the GDPR.

An example of the exercise of enforcement powers by the NDPR against a US business is the advance notification of an administrative fine sent in January 2021 by the NDPA to Grindr LLC for alleged breach of the GDPR (see the answer to question 16.3 above).

## 17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

**17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?**

Unless there is an explicit legal basis for the requested transfer, such a transfer will most likely be deemed to have a purpose which is incompatible with the original purpose for which the data had been collected, thereby necessitating consent from the data subject.

**17.2 What guidance has/have the data protection authority(ies) issued?**

The NDPA has not issued specific guidance on this issue.

## 18 Trends and Developments

**18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.**

In 2020, issues related to the COVID-19 pandemic took centre stage. The NDPA prioritised the investigation of the COVID-19 contact tracing app (see the answer to question 18.2 below), issues related to data protection and digital/online classes/courses for schools and institutions of higher education, as well as issues related to privacy in employment situations.

The NDPA also focused on the school sector and investigated cases of personal data breach (see, for example, the answer to question 16.3 above). Another priority was the health sector where, *inter alia*, the NDPA acted as a sparring partner with regard to the national health analysis platform (*Helseanalyseplattformen*) proposed by the Norwegian Directorate for eHealth.

Furthermore, as the advance notice of an administrative to the US company Grindr LLC shows (see the answer to question 16.3 above), the NDPA has shown its willingness to exercise its powers against businesses established in other jurisdictions.

In 2020, the NDPA continued the trend of 2019, with a record number of personal data breach notifications, totalling 2009. This is slightly higher than last year's record of 1,916 personal data breach notifications.

**18.2 What "hot topics" are currently a focus for the data protection regulator?**

A current "hot topic" since the outbreak of the COVID-19 pandemic in 2020 has been the use of contact tracing to gain control over the spread of the virus in Norway. In Norway, the authorities withdrew the initial contact tracing app that had been launched in April 2020 and launched a new app just before Christmas 2020 that was deemed to be more privacy-friendly.

Another hot issue in 2020 was the launch by the NDPR of a framework for a regulatory sandbox to promote the development and implementation of ethical and responsible artificial intelligence from a privacy perspective. The regulatory sandbox is intended to provide free guidance to a handful of carefully selected companies, of varying types and sizes, across different sectors. Following the first call for applications to take part in the sandbox that closed in January 2021, the NDPR received 25 applications, of which four were chosen – two applicants are from the private sector and the other two are from the public sector. A description of the framework is also available in English on the NDPR's website.

**Gry Hvidsten** is a Partner at Wikborg Rein's Oslo office and Head of the firm's Data Protection practice. She is part of the firm's Technology and Digitalisation practice where she is deputy Head. Hvidsten has been working on data protection issues for close to 20 years, in the Legislation Department of the Ministry of Justice, in Norway's largest company, Equinor, and as a long-time business lawyer.
Gry Hvidsten assists both public and private companies in a variety of industries with questions related to compliance, introduction of new technology and new solutions, privacy in the workplace, whistle-blowing/investigation, digitalisation and digital business, sanctions and GDPR, electronic marketing, big data analytics, GDPR due diligence related to transactions, etc. Hvidsten also assists with agreements related to the processing and sharing of data, including data processing agreements and transfer agreements related to the provision of cloud services. Hvidsten has assisted several international corporations with the implementation of Binding Corporate Rules.
Hvidsten is a frequent speaker at conferences, as well as a lecturer and examiner at the Universities of Bergen and Oslo. She is responsible for several data protection courses offered by *Juristenes utdanningssenter* (the main provider of courses for lawyers in Norway).

**Wikborg Rein Advokatfirma AS**
Dronning Mauds gate 11
0250 Oslo
Norway

Tel: +47 22 82 75 14
Email: ghv@wr.no
URL: www.wr.no/en

**Emily M. Weitzenboeck** has been active in the field of IT law for over 20 years, both as a practitioner and an academic. She is a Senior Lawyer at Wikborg Rein's Oslo office, forming part of the firm's Technology and Digitalisation team, and is an associate professor of law at Oslo Metropolitan University. At Wikborg Rein, she has assisted Norwegian and foreign clients in the public and private sectors, primarily with issues relating to privacy and data protection, e-commerce law, contract law including ICT contracts, marketing law and eHealth law.
Within the field of privacy and data protection, Weitzenboeck has assisted Norwegian and international clients with various questions related to GDPR compliance, and has drafted and quality-assured privacy policies and data processor agreements, among other key texts.
Weitzenboeck was awarded a Ph.D. from the University of Oslo in 2010, has published several works and is a frequent speaker at conferences, as well as a lecturer and examiner at OsloMet, the Norwegian Research Centre for Computers and Law (University of Oslo) and the University of Malta.

**Wikborg Rein Advokatfirma AS**
Dronning Mauds gate 11
0250 Oslo
Norway

Tel: +47 22 82 75 00
Email: emw@wr.no
URL: www.wr.no/en

Wikborg Rein is an international law firm with over 200 lawyers working in our offices in Oslo, Bergen, London, Singapore and Shanghai. Our unique and long-standing presence overseas enables us to offer our clients the benefit of our extensive international expertise.
Wikborg Rein's broad range of legal services includes the following: corporate; dispute resolution; real estate and construction; labour law; banking and finance; shipping and offshore; energy and natural resources; public procurement; intellectual property rights; as well as data protection, digitalisation, information technology and telecommunications.
In the shipping and offshore fields, together with banking and finance, the firm is able to provide services under both Norwegian and English law. The firm has a dedicated team of tax lawyers with notable experience in cross-border taxation matters. In addition, the firm regularly advises on the application of European law, and on all aspects relevant to Norway's position as a member of the EEA.

**www.wr.no/en**

WIKBORG | REIN

# Pakistan


Saifullah Khan


Saeed Hasan Khan

S. U. Khan Associates Corporate & Legal Consultants

## 1 Relevant Legislation and Competent Authorities

### 1.1 What is the principal data protection legislation?

The legislation on data protection is in draft/Bill stage and yet to be passed by Parliament. Its title is the Personal Data Protection Bill, 2020 ("the Bill").

### 1.2 Is there any other general legislation that impacts data protection?

The Prevention of Electronic Crimes Act, 2016 also contains certain significant provisions about data protection.

### 1.3 Is there any sector-specific legislation that impacts data protection?

Within the banking sector, the Payment Systems and Electronic Funds Transfers Act, 2007 provides for the secrecy of financial institutions' customer information; violation is punishable with imprisonment or a financial fine, or both. For the telecoms industry, the Telecom Consumer Protection Regulations, 2009 confer on subscribers of telecoms operators the right to lodge complaints for any illegal practices with the Pakistan Telecommunication Authority, "illegal practices" being a broad term which includes, *inter alia*, illegal use of personal data of subscribers.

### 1.4 What authority(ies) are responsible for data protection?

Under the Bill, the proposed Personal Data Protection Authority of Pakistan would primarily be responsible for data protection.

## 2 Definitions

### 2.1 Please provide the key definitions used in the relevant legislation:

- **"Personal Data"**
  "Personal data" means any information that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession of a data controller, including any sensitive personal data.
  Provided that anonymised, encrypted or pseudonymised data which is incapable of identifying an individual is not personal data.
- **"Processing"**
  "Processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- **"Controller"**
  "Data controller" means a natural or legal person or the government, who either alone or jointly has the authority to make a decision on the collection, obtaining, usage or disclosure of personal data.
- **"Processor"**
  "Data processor" means a natural or legal person or the government who, alone or in conjunction with other(s), processes data on behalf of the data controller.
- **"Data Subject"**
  "Data subject" means a natural person who is the subject of the personal data.
- **"Sensitive Personal Data"**
  "Sensitive personal data" means and includes data relating to access control (username and/or password), financial information such as bank account, credit card, debit card, or other payment instruments, and passports, biometric data, and physical, psychological, and mental health conditions, medical records, and any detail pertaining to an individual's ethnicity, religious beliefs, or any other information for the purposes of this Act and rules made thereunder.
- **"Data Breach"**
  There is no definition of this term in the Bill.
- *Other key definitions*
  - "Pseudonymisation" is the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
  - "Vital interests" means matters relating to life, death or security of a data subject.

## 3 Territorial Scope

**3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?**

Section 3(2) of the Bill is applicable to data controllers and processors not registered or established in Pakistan. Such data controllers and processors are required to nominate a representative in Pakistan.

## 4 Key Principles

**4.1 What are the key principles that apply to the processing of personal data?**

- **Transparency**
  The principle of transparency is not dealt with in the Bill.
- **Lawful basis for processing**
  The collection, processing and disclosure of personal data shall only be carried out in compliance with the provisions of the Bill. Personal data shall not be processed unless processed for a lawful purpose directly related to an activity of the data controller (lawful purpose).
- **Purpose limitation**
  Personal data shall not be processed unless the processing of the personal data is necessary for, or directly related to, lawful purpose.
- **Data minimisation**
  Personal data shall not be processed unless the personal data is adequate, however the personal data must not be excessive in relation to lawful purpose.
- **Proportionality**
  This is not dealt with in the Bill.
- **Retention**
  The Bill stipulates that personal data processed for any purpose shall not be kept longer than is necessary for the fulfilment of that purpose. The Bill confers a duty on the data controller to take all reasonable steps to ensure that all personal data are destroyed or permanently deleted if they are no longer required for the purpose for which they were to be processed.
- **Other key principles**
  The Bill recognises and provides for consent to be an essential requirement to process personal data of the data subject. The Bill also provides that the data controller may not disclose personal data without the consent of the data subject for any purpose other than the purpose for which the same was to be disclosed at the time of collection or to any third party not earlier notified. The Personal Data Protection Authority is to protect personal data from any loss or misuse, to promote awareness of data protection and to deal with complaints.

## 5 Individual Rights

**5.1 What are the key rights that individuals have in relation to the processing of their personal data?**

- **Right of access to data/copies of data**
  The data subject is granted the right of access to personal data, upon payment of a prescribed fee, as to the data subject's personal data that are being processed by or on behalf of the data controller. The data controller must comply with such data access request within 30 days (extendable to an additional 14 days under certain circumstances). The data subject is entitled to:
  - information as to the data subject's personal data that are being processed by or on behalf of the data controller; and
  - have communicated to him a copy of the personal data in an intelligible form.
- **Right to rectification of errors**
  In the case that personal data have been supplied to the data subject upon his request and the same are inaccurate, incomplete, misleading or not up to date, or when the data subject knows that his personal data are inaccurate, incomplete, misleading or not up to date, the data subject has the right to get them corrected by making a written request to the data controller.
- **Right to deletion/right to be forgotten**
  The data subject has the right to request that the data controller, without undue delay, erase personal data in the following situations:
  - the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
  - the data subject withdraws the consent on which the processing is based;
  - the data subject objects to the processing;
  - the personal data have been unlawfully processed; or
  - the personal data must be erased for compliance with a legal obligation.
- **Right to object to processing**
  The data subject has the right to give "data subject notice" in writing to the data controller to:
  (i) cease the processing, or processing for a specified purpose or in a specified manner; or
  (ii) not begin the processing, or processing for a specified purpose or in a specified manner.
  The data subject must state reasons in the "data subject notice" that:
  (i) the processing of that personal data or the processing of personal data for that purpose or in that manner is causing, or is likely to cause, substantial damage or distress to him or to another person; and
  (ii) the damage or distress is, or would be, unwarranted.
- **Right to restrict processing**
  As explained above.
- **Right to data portability**
  There is no such right in the Bill.
- **Right to withdraw consent**
  The data subject has the right to withdraw his consent.
- **Right to object to marketing**
  The data subject has the right to give "data subject notice" in writing to the data controller to:
  (i) cease the processing, or processing for a specified purpose or in a specified manner; or
  (ii) not begin the processing, or processing for a specified purpose or in a specified manner.
  The data subject must state reasons in the "data subject notice" that:
  (i) the processing of that personal data or the processing of personal data for that purpose or in that manner is causing, or is likely to cause, substantial damage or substantial distress to him or to another person; and
  (ii) the damage or distress is, or would be, unwarranted.
- **Right to complain to the relevant data protection authority(ies)**
  The data subject may file a complaint before the proposed Personal Data Protection Authority of Pakistan against

any violation of personal data protection rights as granted under the Bill, regarding the conduct of any data controller, data processor or their processes which the data subject regards as involving:
(i) a breach of the data subject's consent to process data;
(ii) a breach of obligations of the data controller or the data processor in the performance of their functions under the Bill;
(iii) the provision of incomplete, misleading or false information while taking consent of the data subject; or
(iv) any other matter relating to protection of personal data.

- **Other key rights**
None other than the above.

## 6 Registration Formalities and Prior Approval

**6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?**

There is no expressed requirement in the Bill; however, while discussing the power of the Personal Data Protection Authority of Pakistan, the Bill confers upon it the power to devise a registration mechanism for data controllers and data processors. Therefore, the proposed Personal Data Protection Authority of Pakistan, when established, will devise the registration requirements.

**6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?**

This aspect will be addressed under the rules to be framed by the proposed Personal Data Protection Authority of Pakistan (please see question 6.1 above).

**6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?**

This aspect will be addressed under the rules to be framed by the proposed Personal Data Protection Authority of Pakistan (please see question 6.1 above).

**6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?**

This aspect will be addressed under the rules to be framed by the proposed Personal Data Protection Authority of Pakistan (please see question 6.1 above).

**6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?**

This aspect will be addressed under the rules to be framed by the proposed Personal Data Protection Authority of Pakistan (please see question 6.1 above).

**6.6 What are the sanctions for failure to register/notify where required?**

This aspect will be addressed under the rules to be framed by the proposed Personal Data Protection Authority of Pakistan (please see question 6.1 above).

**6.7 What is the fee per registration/notification (if applicable)?**

This aspect will be addressed under the rules to be framed by the proposed Personal Data Protection Authority of Pakistan (please see question 6.1 above).

**6.8 How frequently must registrations/notifications be renewed (if applicable)?**

This aspect will be addressed under the rules to be framed by the proposed Personal Data Protection Authority of Pakistan (please see question 6.1 above).

**6.9 Is any prior approval required from the data protection regulator?**

This aspect will be addressed under the rules to be framed by the proposed Personal Data Protection Authority of Pakistan (please see question 6.1 above).

**6.10 Can the registration/notification be completed online?**

This aspect will be addressed under the rules to be framed by the proposed Personal Data Protection Authority of Pakistan (please see question 6.1 above).

**6.11 Is there a publicly available list of completed registrations/notifications?**

This aspect will be addressed under the rules to be framed by the proposed Personal Data Protection Authority of Pakistan (please see question 6.1 above).

**6.12 How long does a typical registration/notification process take?**

This aspect will be addressed under the rules to be framed by the proposed Personal Data Protection Authority of Pakistan (please see question 6.1 above).

## 7 Appointment of a Data Protection Officer

**7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.**

There is no expressed requirement in the Bill; however, while discussing the power of the Personal Data Protection Authority

of Pakistan, the Bill confers upon it the power to formulate responsibilities of the Data Protection Officer. Therefore, the proposed Personal Data Protection Authority of Pakistan, when established, will devise the appointment requirements.

**7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?**

In view of question 7.1 above, this is not applicable.

**7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?**

In view of question 7.1 above, this is not applicable.

**7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?**

In view of question 7.1 above, this is not applicable.

**7.5 Please describe any specific qualifications for the Data Protection Officer required by law.**

In view of question 7.1 above, this is not applicable.

**7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?**

In view of question 7.1 above, this is not applicable.

**7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?**

In view of question 7.1 above, this is not applicable.

**7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?**

In view of question 7.1 above, this is not applicable.

## 8 Appointment of Processors

**8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?**

The Bill is silent on this aspect; however, businesses customarily execute an agreement to this effect.

**8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?**

It is not necessary, under the Bill, to enter into an agreement. However, for the enforcement of an agreement, such formalities must be summarised in writing and registered under the Registration Act, 1908.

## 9 Marketing

**9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).**

No such legislative restriction exists.

**9.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?**

No such legislative restriction exists.

**9.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).**

No such legislative restriction exists.

**9.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?**

No such legislative restriction exists.

**9.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?**

For the time being, there is no data protection authority in existence.

**9.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?**

There is no law regulating this mechanism as such.

**9.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?**

None, as there is no legislation to this effect.

## 10 Cookies

**10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).**

No such legislative restriction exists.

**10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?**

No such legislative restriction exists.

**10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?**

None, in view of there not being any legislation to this effect, and the fact that no data protection authority exists.

**10.4 What are the maximum penalties for breaches of applicable cookie restrictions?**

None, in view of there not being any legislation to this effect.

## 11 Restrictions on International Data Transfers

**11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.**

The Bill provides that if personal data is required to be transferred to any system located beyond the territories of Pakistan or any system that is not under the direct control of any of the governments in Pakistan, it must be ensured that the country where the data is being transferred offers personal data protection at least equivalent to the protection provided under the Bill. The personal data so transferred shall be processed in accordance with the Bill. Critical personal data shall only be processed in Pakistan. The Federal Government is vested with the power to exempt certain categories of personal data (except sensitive data) from these requirements on the grounds of necessity or strategic interests.

**11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).**

There are no such mechanisms.

**11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.**

This is not yet specified in the Bill, although it may be a subject matter of the rules to be framed thereunder.

**11.4 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?**

This is not applicable.

**11.5 What guidance (if any) has/have the data protection authority(ies) issued in relation to the European Commission's revised Standard Contractual Clauses?**

This is not applicable.

## 12 Whistle-blower Hotlines

**12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?**

The Bill does not have any provision related to "whistle-blower". The Public Interest Disclosures Act, 2017 deals with the concept of "whistler-blower"; however, the same primarily deals with and focuses on public sector entities. The said Act has mandated the Government to specify private sector entities (in the official *Gazette*) to be an "organisation" for the purposes of said Act. Primarily, the Public Interest Disclosures Act, 2017 covers the wilful misuse of power or wilful misuse of discretion by virtue of which substantial loss is caused to the Government or substantial wrongful gain accrues to a public servant or to a third party. As such, the corporate sector is not the subject matter of the Public Interest Disclosures Act, 2017.

**12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?**

The Bill is silent on this matter, however, anonymous or pseudonymous disclosures are not entertained in terms of Section 3(5) of the Public Interest Disclosures Act, 2017.

## 13 CCTV

**13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?**

The Bill does not place or require any registration/notification or prior approval in relation to the use of CCTV.

**13.2 Are there limits on the purposes for which CCTV data may be used?**

There are no such limits (please see question 13.1 above).

## 14 Employee Monitoring

**14.1 What types of employee monitoring are permitted (if any), and in what circumstances?**

The Bill does not have any provision regarding employee monitoring.

**14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.**

The Bill does not have such requirement. However, consent is generally built-in within the employment contract.

**14.3 To what extent do works councils/trade unions/ employee representatives need to be notified or consulted?**

There is no such requirement.

## 15 Data Security and Data Breach

**15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?**

Data controllers, under the Bill, are responsible for taking practical steps to protect personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction.

**15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

The Bill requires the data controller to report a data breach to the Personal Data Protection Authority of Pakistan within 72 hours. The exception is where the personal data breach is unlikely to result in a risk to the rights and freedoms of the data subject.

In case the notification is made beyond 72 hours, the notification is to state reasons for the delay.

The notification must contain the following information:

- Description of the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned.
- Name and contact details of the Data Protection Officer or other contact point where more information can be obtained.
- Likely consequences of the personal data breach.
- Measures adopted or proposed to be adopted by the data controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

**15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

There is no such requirement in the Bill.

**15.4 What are the maximum penalties for data security breaches?**

| Breach | Penalty |
|---|---|
| A data controller not ceasing the processing of personal data after withdrawal of consent by the data subject. | Fine of up to PKR 5 million (US$ 31,500 approx.) or imprisonment for a term not exceeding three years or both. |
| Anyone who processes or cause to be processed, disseminates or discloses personal data in violation of this Act. | Fine of up to PKR 15 million (US$ 95,000 approx.) and in case of a subsequent unlawful processing the fine may be raised up to PKR 25 million (US$ 158,000 approx.). In certain cases, the fine may be raised to PKR 25 million (US$ 158,000 approx.). |
| Failure to adopt the security measures that are necessary to ensure data security. | Fine of up to PKR 5 million (US$ 31,500 approx.). |
| Failure to comply with the orders of the Personal Data Protection Authority of Pakistan or the court. | Fine of up to PKR 2.5 million (US$ 15,800 approx.). |

## 16 Enforcement and Sanctions

**16.1 Describe the enforcement powers of the data protection authority(ies).**

(a) **Investigative powers**: The Personal Data Protection Authority of Pakistan shall have the powers to decide a complaint, under the Bill, and shall be deemed to be a Civil Court and shall have the same powers as are vested in a Civil Court.

(b) **Corrective powers**: The Personal Data Protection Authority of Pakistan shall have the powers to order a data controller to take such reasonable measures as it may deem necessary to remedy an applicant for any failure to implement the provisions of the Bill. In addition, it shall have the powers to take prompt and appropriate action in response to a data security breach.

(c) **Authorisation and advisory powers**: Advising to the Federal Government and any other statutory authority on measures that must be undertaken to promote protection of personal data and ensuring consistency of application and enforcement of the Bill, shall be one of the functions entrusted upon the Personal Data Protection Authority of Pakistan.

(d) **Imposition of administrative fines for infringements of specified GDPR provisions**: The Personal Data Protection Authority of Pakistan shall have the powers to impose penalties for non-compliance of the provisions of the Bill.

(e) **Non-compliance with a data protection authority**: The Personal Data Protection Authority of Pakistan shall have the powers to impose a fine of up to Rs. 2.5 Million (US$ 15,800 approx.) in case anyone fails to comply with its orders.

**16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?**

The Bill is silent on this.

**16.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.**

As the Personal Data Protection Authority of Pakistan is not in existence, there is nothing to state regarding its approach, nor are there any cases as of yet.

**16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?**

This is not applicable (please see question 16.3 above).

## 17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

**17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?**

The Bill is silent on this aspect; however, generally the foreign law enforcement agencies do not communicate with businesses directly; rather, businesses are contacted via the relevant law enforcement agencies of Pakistan, who coordinate with businesses to respond to foreign law enforcement agencies.

**17.2 What guidance has/have the data protection authority(ies) issued?**

As the Personal Data Protection Authority of Pakistan is not in existence, no such guidelines exist.

## 18 Trends and Developments

**18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.**

There are no enforcement trends that have emerged in Pakistan over the last 12 months.

**18.2 What "hot topics" are currently a focus for the data protection regulator?**

As the Personal Data Protection Authority of Pakistan is non-existent for the time being, once it comes into force, e-Commerce, banking transactions and telecoms are likely to be the "hot topics" on which the Authority is expected to focus.

**Saifullah Khan** is an international trade, IT and policy lawyer, with 20 years' experience in international trade policy and law advisory, serving a large client base in the domestic and international market. He is a very successful and renowned anti-dumping lawyer not only in Pakistan but in various jurisdictions due to his rich experience and expertise in Trade Defense Laws of the World Trade Organization. He has been engaged in more than 85% of the anti-dumping investigations initiated by the Pakistani Antidumping Authority (i.e. National Tariff Commission, Ministry of Commerce) to this day, and has been providing trade remedial consultancy services to the domestic industry in Pakistan as well as a large number of foreign producers/exporters in various countries. Mr. Khan has been writing and presenting papers on International Trade laws, Competition law, Dispute Settlement, Preferential Trade Agreements, Data Protection & e-Commerce, Trade in Services, etc. Additionally, to keep himself up-to-date with respect to the development of trade and other related policies, Mr. Khan completed an Executive Education Program on "Mastering Trade Policy" from Harvard Kennedy School, Boston, USA. He is an Advocate of the High Court, a Fellow Member of the Institute of Cost & Management Accountants of Pakistan and a Member of the Chartered Institute of Arbitrators (UK).

**S. U. Khan Associates Corporate & Legal Consultants**
First Floor, 92 Razia Sharif Plaza
Fazal-ul-Haq Road, Blue Area
Islamabad, 44000
Pakistan

Tel: +92 51 23447 41/42
Email: saifullah.khan@sukhan.com.pk
URL: www.sukhan.com.pk

**Saeed Hasan Khan** has vast experience of advising clients on various issues such as taxation, corporate, regulatory compliance, contractual obligations etc. and representing them before the authorities. Over the past 20 years, he has practised in direct and indirect taxes, which encompasses all three practice tiers: advisory; execution; and litigation. He advises on cross-border transactions, international tax treaties and matters related to tax due diligence, corporate structures, shareholder agreements and contractual stipulations between the companies. He has developed a keen professional interest in emerging laws about personal data protection and has gained a deep understanding of underlying concepts and principles governing the global data protection laws including the General Data Protection Regulation of the European Union. He carried out a great deal of research on personal data protection laws in various jurisdictions to have a comparison of core legal principles in various jurisdictions.

**S. U. Khan Associates Corporate & Legal Consultants**
First Floor, 92 Razia Sharif Plaza
Fazal-ul-Haq Road, Blue Area
Islamabad, 44000
Pakistan

Tel: +92 51 23447 41/42
Email: saeed.hasan@sukhan.com.pk
URL: www.sukhan.com.pk

S. U. Khan Associates Corporate & Legal Consultants is a pioneering and leading firm practising trade remedy law in Pakistan, with local and international clients. The major service areas include International Trade laws, Data Protection & e-Commerce & IT Laws, Competition Law, Foreign Investment Advisory Services, and International Trade Agreements Advisory. The Firm is also a great contributor to the dissemination of professional knowledge in various journals as well as international institutions, such as the United Nations Conference on Trade and Development and the United Nations Commission on International Trade Law (UNCITRAL), etc. The partners have been working closely with the Government in drafting legislations and in policy-making.

**www.sukhan.com.pk**

S.U.Khan Associates
Corporate & Legal Consultants

# Peru


Erick Iriarte Ahón


Fátima Toche Vega

Iriarte & Asociados

## 1 Relevant Legislation and Competent Authorities

### 1.1 What is the principal data protection legislation?

Data protection in Peru is governed by Law No. 29733 (Law on Personal Data Protection), published in the Official Gazette on 3 July 2011, and Supreme Decree No. 003-2013-JUS, which approved the Regulations under the Law on Personal Data Protection, published in the Official Gazette on 22 March 2013. The Law on Personal Data Protection entered into force on 4 July 2011; however, many of the provisions and its Regulations became effective on 8 May 2013. The Peruvian Constitutional Procedural Code recognises the habeas data process, which defends the constitutional right to personal data protection. In 2017, Legislative Decree No.1353 (DL 1353) made modifications to the Law on Personal Data Protection.

### 1.2 Is there any other general legislation that impacts data protection?

The Law regulating private risk information registries and providing protection to the owners of information is Law No. 27489, which is modified by Law No. 27863. Article 207-D of the Peruvian Criminal Code penalises the illicit traffic of data. Furthermore, Urgency Decree 007-2020 (DU 007-2020) approves the digital trust framework and provides measures for its strengthening.

### 1.3 Is there any sector-specific legislation that impacts data protection?

This is the Finance Regulation for Information Security and Cybersecurity (Resolution SBS N° 504-2021).

### 1.4 What authority(ies) are responsible for data protection?

The authority responsible for overseeing the data protection law is the Peruvian Data Protection Authority (APDP); this entity is attached to the Ministry of Justice.

## 2 Definitions

### 2.1 Please provide the key definitions used in the relevant legislation:

- "**Personal Data**"
  This is defined as any information on an individual which identifies or makes him identifiable through means that may be reasonably used.
- "**Processing**"
  This is defined as any operation or technical procedure, automated or not, that permits compiling, registration, organisation, storage, conservation, preparation, modification, extraction, consultation, utilisation, blockage, suppression, communication by transfer or distribution or any other form of processing that facilitates the access, correlation or interconnection of personal data.
- "**Controller**"
  This is defined as the individual, private legal person or public entity that determines the purpose and content of the personal data database, their processing and the security measures.
- "**Processor**"
  Data processors are the natural persons or legal entities, private or public, that process personal data on behalf of data controllers by virtue of a legal relationship that binds them and delineates their scope of activity.
- "**Data Subject**"
  This is defined as the individual to whom the personal data belong.
- "**Sensitive Personal Data**"
  This is defined as personal data consisting of: biometric data; data concerning racial and ethnic origin; political, religious, philosophical or moral opinions or convictions; personal habits; union membership; economic income; and information related to health or sexual life.
- "**Data Breach**"
  This is not defined in the Law on Personal Date Protection; however, DU 007-2020 includes a definition of a "Digital security incident" as an "[e]vent or series of events that can compromise trust, economic prosperity, the protection of people and their personal data, information, among other assets of the organization, through digital technologies".
- *Other key definitions – please specify (e.g., "Pseudonymous Data", "Direct Personal Data", "Indirect Personal Data")*
  Anonymisation procedure: Anonymisation is an irreversible procedure that either prevents identification or does not make any data subject identifiable.

Dissociation procedure: Dissociation is a reversible procedure that either prevents identification or does not make any data subject identifiable.
Database: A database is an organised set of personal data, automated or not, and regardless of the support. It may be physical, magnetic, digital, optical, among others. Furthermore, the form of its creation, storage, organisation and access is irrelevant.

## 3 Territorial Scope

**3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?**

The Law on Personal Data Protection applies to the personal data contained or intended to be contained in personal data databases publicly and privately administered and/or processed in Peru. The law only states that contractual clauses are established to determine the same level of protection as in Peruvian law.

## 4 Key Principles

**4.1 What are the key principles that apply to the processing of personal data?**

- **Transparency**
  This is not applicable to Peru.
- **Lawful basis for processing**
  The processing of personal data will be carried out according to the provisions of the law. Compiling personal data by fraudulent, unfair or illegal means is prohibited.
- **Purpose limitation**
  Personal data must be compiled for a determined, explicit and legal purpose. Personal data processing must not be extended for a purpose other than that established unequivocally as such at the time of compiling, excluding the cases of activities with historical, statistical or scientific value when using a dissociation or anonymisation procedure.
- **Data minimisation**
  This is not applicable to Peru.
- **Proportionality**
  Any personal data processing must be adequate, relevant and non-excessive for the purpose for which the data were compiled.
- **Retention**
  This is not applicable to Peru.
- *Other key principles – please specify*
  Principle of consent: The data subject must give his consent for the processing of personal data.
  Principle of quality: Personal data to be processed must be truthful, accurate and, as far as possible, updated, necessary, pertinent and adequate for the purpose for which they were compiled. They must be kept in such a way as to guarantee their security and only for the time necessary to achieve the purpose of the processing.
  Principle of security: The personal data database controller and the data processor must adopt the necessary technical and organisational measures to guarantee the security of the personal data. Security measures must be appropriate and in line with the processing to be carried out and the category of personal data in question.
  Adequate level of protection: For cross-border data transfers, the person responsible for the processing must ensure a sufficient level of protection for personal data, which must be at least comparable to the provisions of the Law on Personal Data or international standards.

## 5 Individual Rights

**5.1 What are the key rights that individuals have in relation to the processing of their personal data?**

- **Right of access to data/copies of data**
  The data subject has the right to access personal data that is subject to processing in databases and obtain information regarding the way the data was compiled, the reasons for the compilation, at whose request the compilation was made, and the transfers carried out or to be carried out.
  The responsible may deny access to data in the following instances: in order to protect the rights and interests of third parties; where it would prevent pending judicial or administrative proceedings; where it is related to the investigation of compliance with tax or social security obligations, the performance of health and environmental control functions, or the verification of administrative violations; or when ordered so by law.
- **Right to rectification of errors**
  The data subject has the right to the update, inclusion, rectification and elimination of his personal data processed when they are partially or totally inaccurate, incomplete, when noticing omission, error or inaccuracy, when they are no longer necessary or relevant for the purpose for which they were compiled, or upon the expiration of the term established for their processing.
  If his personal data were previously transferred, the personal data database controller must communicate the update, inclusion, rectification and/or elimination to the party to whom they were transferred, if the latter continues processing them, and the latter must also proceed with the update, inclusion, rectification and/or elimination, as the case may be.
- **Right to deletion/right to be forgotten**
  Please see right to rectification of errors above.
- **Right to object to processing**
  The data subject has the right to prevent the data from being supplied, especially when it affects his fundamental rights.
- **Right to restrict processing**
  Please see right to object to processing above.
- **Right to data portability**
  This is not applicable to Peru.
- **Right to withdraw consent**
  The data subject may revoke his consent at any time with the obligation to support his request when applicable, complying in this regard with the same requisites as when he gave his consent.
- **Right to object to marketing**
  This is not applicable to Peru.
- **Right to complain to the relevant data protection authority(ies)**
  Any data subject must have the administrative and/or jurisdictional channels necessary to claim and enforce his rights when they are violated by the processing of his personal data.
- *Other key rights – please specify*
  - **Principle of adequate level of protection**: In the case of transborder personal data flow, the receiving country must have a sufficient level of protection for the personal data to be processed or at least comparable to that provided by the Law on Personal Data Protection.

The sufficient protection scope of the receiving country must include at least the consignment and compliance with the guiding principles previously mentioned.

## 6 Registration Formalities and Prior Approval

**6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?**

Businesses and processors of personal data are required to register personal data databases.

**6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?**

The registration must be specific.

**6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?**

Registrations are made by database.

**6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?**

All natural person and organisations, whether public or private, who manage data information in Peru must register with the APDP.

**6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?**

The following information must be included in the registration: details of the entity; affected categories; affected categories of personal data; processing purposes; and international transfer of data.

**6.6 What are the sanctions for failure to register/notify where required?**

Failure to register could be considered serious misconduct with a financial penalty fine of up to 50 tax units (approx. €55,500).

**6.7 What is the fee per registration/notification (if applicable)?**

The fee per registration is approx. €11.50 per database.

**6.8 How frequently must registrations/notifications be renewed (if applicable)?**

The frequency at which registrations must be renewed will be determined on a case-by-case basis.

**6.9 Is any prior approval required from the data protection regulator?**

No, prior approval is not required from the data protection regulator.

**6.10 Can the registration/notification be completed online?**

Currently, registration cannot be completed online.

**6.11 Is there a publicly available list of completed registrations/notifications?**

Yes, please see: https://prodpe.minjus.gob.pe/prodpe_web/BancoDato_verResultado.

**6.12 How long does a typical registration/notification process take?**

A typical registration process takes eight weeks.

## 7 Appointment of a Data Protection Officer

**7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.**

The appointment of a Data Protection Officer is optional.

**7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?**

This is not applicable to Peru.

**7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?**

This is not applicable to Peru.

**7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?**

This is not applicable to Peru.

**7.5 Please describe any specific qualifications for the Data Protection Officer required by law.**

This is not applicable to Peru.

**7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?**

This is not applicable to Peru.

**7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?**

This is not applicable to Peru.

**7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?**

This is not applicable to Peru.

## 8 Appointment of Processors

**8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?**

The processing of personal data may be carried out by a third party other than the data processor through an agreement or contract between the two.

In this case, prior authorisation will be required from the owner of the personal data bank or data controller. Such authorisation shall also be deemed to have been granted if it was provided for in the legal instrument by which the relationship between the data controller and the data processor was formalised. The processing carried out by the subcontractor shall be carried out in the name and on behalf of the controller; however, the burden of proving the authorisation rests with the processor.

**8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?**

There is no express provision in the Law on Personal Data Protection or the Regulation that obliges data controllers to enter into written agreements with data processors. Nevertheless, the Regulation suggests that written agreements may be a good mechanism to oblige data processors to assume all the obligations imposed by legislation and, thus, to ensure that the personal information will be processed according to the Law on Personal Data Protection, the Regulation, and the conditions under which data subjects authorised the processing of their information.

Therefore, it is highly recommended to enter into written agreements that rule the legal relationship between both parties, and to include provisions according to which data processors are obliged to comply with all the provisions contained in Peruvian legislation. It is important to note that these agreements must determine the scope of the processing and the responsibilities of data processors.

## 9 Marketing

**9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).**

The Peruvian Consumer Code establishes as "Aggressive" or "Deceptive Commercial Methods" the use of: call centres; telephone call systems; sending text messages to cell phones or mass electronic messages to promote products and services; and providing telemarketing services to all those telephone numbers and email addresses of consumers who have not given the suppliers of such goods and services their prior, informed, express and unequivocal consent for the use of this commercial practice.

**9.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?**

These restrictions are only applicable to business-to-consumer marketing.

**9.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).**

Law 28493 (the Spam Act) was enacted on April 12 2005, to regulate the use of unsolicited commercial emails, commonly known as spam. Supreme Decree No. 031-2005-MTC is the implementing regulation for the Spam Act, issued by the Ministry of Transportation and Communications on January 4 2006. The National Institute for Defense of Competition and Protection of Intellectual Property (INDECOPI) is the competent agency for enforcing the Spam Act regulations. The Spam Act empowers the Peruvian Commission for Consumer Protection and INDECOPI to set fines according to the law on consumer protection and the standard for advertising to defend the consumer.

**9.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?**

No; the restrictions noted above do not apply to marketing sent from other jurisdictions.

**9.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?**

No; INDECOPI is the authority in charge of the enforcement of breaches of marketing restrictions.

**9.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?**

Yes, it is lawful; however, the data subject must have authorised that data transfer, and also the data must have been collected according to the Law on Personal Data Protection.

**9.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?**

- For minor infringements: fines of up to 50 tax units (approx. €5,550);
- For serious infringements: fines of up to 100 tax units (approx. €55,500); and
- For very serious infringements: fines of up to 450 tax units (approx. €111,000).

## 10 Cookies

**10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).**

Cookies are understood by the APDP as personal data, and are thus applicable to the principles of the Law on Personal Data Protection.

**10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?**

No; the applicable restrictions do not distinguish between different types of categories.

**10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?**

No; the APDP has not taken any enforcement action in relation to cookies to date.

**10.4 What are the maximum penalties for breaches of applicable cookie restrictions?**

- For minor infringements: fines of up to five tax units (approx. €5,550);
- for serious infringements: fines of up to 50 tax units (approx. €55,500); and
- for very serious infringements: fines of up to 100 tax units (approx. €111,000).

## 11 Restrictions on International Data Transfers

**11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.**

According to the Law on Personal Data Protection, data controllers are obliged to register their personal databases in the National Registry. Likewise, cross-border transfers of personal data must be notified to the APDP.

**11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).**

The mechanisms that businesses typically utilise to transfer personal data abroad include: consent of the data subject; approved contractual clauses; compliance with legal obligations; and financial transfers. The performance of a contract with the data subject is included as an exception from specific consent under data protection law; however, the subject must be informed of this.

**11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.**

Cross-border transfers of personal data must only be notified to the APDP.

**11.4 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?**

This is not applicable to Peru.

**11.5 What guidance (if any) has/have the data protection authority(ies) issued in relation to the European Commission's revised Standard Contractual Clauses?**

This is not applicable to Peru.

## 12 Whistle-blower Hotlines

**12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?**

Peru does not have specific regulation regarding this.

**12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?**

While anonymous reporting is generally permitted, Peru does not have specific regulation regarding this.

## 13 CCTV

**13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?**

Under the Law on Personal Data Protection, CCTV records must be registered as a database; however, prior approval is not required. The specific regulation can be found here: https://www.minjus.gob.pe/wp-content/uploads/2020/01/Directiva-N%C2%B0-01-2020-DGTAIPD-1.pdf.

**13.2 Are there limits on the purposes for which CCTV data may be used?**

Regarding the limits on the purposes for which CCTV data may

be used, it is imperative to follow the Law on Personal Data Protection and the Regulation.

## 14 Employee Monitoring

**14.1 What types of employee monitoring are permitted (if any), and in what circumstances?**

Communications, telecommunications, computer systems or their instruments, both public and private, can only be opened, seized or intercepted by order of the judge, with permission from the owner and with the guarantees provided for in the law. Any personal data obtained in violation of this mandate has no legal effect.

According to the Video Surveillance Directive, personal data of employees obtained through video surveillance systems must be kept for a maximum of 30 to 60 days. In case such data proves the commission of a labour misconduct, they can be kept for up to 120 days. Otherwise, retention of such data requires the express consent of employees.

In addition, labour regulations and tax regulations establish some data retention obligations for employees, which depend on the type of information.

According to Article 87 of the Peruvian Tax Code, employers are obliged to keep the documents connected to the payments of social benefits and taxes of employees for a period of 10 years.

According to Article 28 of Law No. 29783 (Law on Occupational Health and Safety), records of occupational diseases of employees must be kept for a period of 20 years, the records of work accidents and dangerous incidents for a period of 10 years after the event, and other records for a period of five years after the event.

**14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.**

Obtaining consent is recommended. Employers typically include in contracts specific clauses about monitoring.

**14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?**

This is not applicable to Peru.

## 15 Data Security and Data Breach

**15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?**

The general rules are included in the Directive of Security of Personal Data: please see https://www.minjus.gob.pe/wp-content/uploads/2014/02/Cartilla-de-Directiva-de-Seguridad.pdf. Furthermore, DU 007-2020 includes some obligations in case of data breach.

**15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

DU 007-2020 includes reports to the APDP and National Center of Digital Trust. However, the procedure is not approved yet.

**15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

Please see question 15.2 above.

**15.4 What are the maximum penalties for data security breaches?**

The maximum penalties for security breaches are not defined.

## 16 Enforcement and Sanctions

**16.1 Describe the enforcement powers of the data protection authority(ies).**

(a) **Investigative Powers**: the power to investigate complaints lodged by data subjects and issue provisional or corrective measures as established in the Regulation; start investigations, *ex officio* or following a complaint from a party for presumed acts contrary to the provisions of the Law on Personal Data Protection and apply the corresponding administrative sanctions; answer questions regarding personal data protection and the meaning of the current rules; issue corresponding guidelines for the better application of the Law on Personal Data Protection and its Regulation; and cooperating with foreign data protection authorities and generating bilateral and multilateral cooperation mechanisms for mutual assistance and help when required.

(b) **Corrective Powers**: the supervision of the personal data processing carried out by data controllers and data processors and, in the case of illegal acts, the power to order the appropriate actions pursuant to the Law on Personal Data Protection.

(i) Minor infringements include:
- processing personal data without adopting security measures;
- collecting personal data that is not necessary, relevant, or appropriate regarding the purposes for which it had been obtained;
- not replying to, impeding, or obstructing the exercise of data subjects' rights; and
- obstructing the APDP's audits.

(ii) Serious infringements include:
- processing personal data without the data subject's consent;
- processing personal data while not fulfilling the Law's principles;
- not complying with the obligation of confidentiality;
- not replying to, impeding or obstructing, in a systematic way, the exercise of data subjects' rights; and
- obstructing, in a systematic way, the APDP's audits.

(iii) Very serious infringements include:
- when the processing of personal data does not comply with the Law on Personal Data Protection's principles and this circumstance impedes or obstructs the exercise of data subjects' rights;

- creating, modifying or cancelling a database without complying with the Law on Personal Data Protection;
- giving false documents or information to the APDP;
- not ceasing the unlawful processing of personal data when this was previously required; and
- not registering the personal database despite having been required by the APDP to do so.

(c) **Authorisation and Advisory Powers**: the administration and maintenance of the National Registry; answer questions regarding personal data protection and the meaning of the current rules; issue corresponding guidelines for the better application of the Law on Personal Data Protection and its Regulation.

(d) **Imposition of administrative fines for infringements of specified GDPR provisions**: the data protection authority is entitled to impose the following sanctions:
(i) for minor infringements: fines of up to five tax units (approx. €5,550);
(ii) for serious infringements: fines of up to 50 tax units (approx. €55,500); and
(iii) for very serious infringements: fines of up to 100 tax units (approx. €111,000).

(e) **Non-compliance with a data protection authority:** This is not applicable to Peru.

**16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?**

This is not included in the Law on Personal Data Protection directly.

**16.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.**

The APDP has already conducted several preliminary investigations in accordance with its supervising powers and has imposed penalties for failure to comply with the legal framework. Despite most of the cases being a consequence of not having complied with the registration of databases requirement, the APDP's decision against *Supermercados Peruanos* S.A. is of particular relevance since it referred to the principles of consent, security, and adequate levels of protection.

In particular, *Supermercados Peruanos*, which owns several supermarket chains in Peru such as *Plaza Vea* and *Vivanda*, collected personal data from its clients in order to send them advertisements of its products and services. In 2016, by means of an audit, the APDP became aware of several violations of the Law on Personal Data Protection committed by *Supermercados Peruanos*. The APDP found that *Supermercados Peruanos* had failed to inform data subjects of the recipients of their personal data, implement security measures, and communicate to the APDP that it had transferred data outside Peruvian territory, which was in violation of the principles of consent, security, and adequacy. The APDP imposed a fine amounting to 8.5 tax units, which is equivalent to approximately PEN 36,550 (approx. €9,430).

Please note that the Law on Personal Data Protection provides that data controllers must process personal data with the free, prior, informed, express and unequivocal consent of data subjects. It also states that they must implement security measures for the protection of personal data collected in order to prevent loss or unauthorised access by third parties. Finally, it provides that data controllers must register any cross-border flow of personal data carried out with the APDP. According to the APDP, the prosecuted company breached these obligations.

Additionally, in 2019, the APDP issued a decision against the National Office of Electoral Processes (ONPE) due to the massive exposure of voters' personal data through the web platform, "Hackathon". The APDP determined that, since the ONPE did not guarantee the security of the data against unauthorised access, it had violated the principle of security established in the Law on Personal Data Protection as well as some provisions of the Security Directive. The APDP found that the infringement was minor and therefore imposed a fine of one tax unit, which is equivalent to approximately PEN 4,300 (approx. €1,110). This case is of particular relevance since a public entity was sanctioned.

**16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?**

The APDP does not exercise its powers established in other jurisdictions directly.

## 17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

**17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?**

This is not applicable to Peru.

**17.2 What guidance has/have the data protection authority(ies) issued?**

This is not applicable to Peru.

## 18 Trends and Developments

**18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.**

Recent enforcement trends that have emerged during the past 12 months include Data Analysis, Health Information related to COVID-19 and facial recognition.

**18.2 What "hot topics" are currently a focus for the data protection regulator?**

There is currently a special focus on health data related to COVID-19 (such as temperature controls, infected tracing, contact tracing).

**Erick Iriarte Ahón** is Partner of Iriarte & Asociados and has obtained a Master's in Political Science and Government with a mention in Public Policies and Public Management (PUCP). Erick is the CEO of eBIZ and was the first General Manager of LACTLD, an association of ccTLDs in Latin America. Furthermore, Erick was delegated by Peru to coordinate the Working Group on the Regulatory Framework of the Information Society and Internet Governance of the eLAC Platform. He has also been the coordinator of the Goal on the Information Society Regulatory Framework of the eLAC Plan since 2005. In addition, Erick is Legal Advisor to the Administration of Domain Names .pe (ccTLD .pe) and Deputy Director of the APEC E-Commerce Business Alliance (APEC-ECBA). He was a member of the Internet Governance Forum – MAG, a team formed to advise the United Nations Secretary for the IGF. Moreover, he has been a member of the Advisory Council of .ORG. He has been Vice-Chair of the At-Large Advisory Committee of ICANN, where he was also a delegate to the NCUC and a Member of the ICANN Fellowship Committee. Erick is a Member of the International Advisory Committee of the ccTLD .pr and the ccTLD .ni., web editor of the LatinoamerICANN Project on Internet Governance in Latin America, as well as Executive Director of Alfa-Redi.

**Iriarte & Asociados**
Calle Enrique Palacios N° 360, office 612
Miraflores
Lima
Peru

Tel: +51 99 966 6544
Email: eiriarte@iriartelaw.com
URL: www.iriartelaw.com

**Fátima Toche Vega** is Legal Head of Iriarte & Asociados and a lawyer from the Pontifical Catholic University of Peru, as well as a member of the Lima Bar Association. Fátima received a postgraduate degree in Regulation and Dispute Resolution in International Trade and Investments from the University of Buenos Aires, as well as a Master's in International Business Management from the School of Industrial Organization (EOI) of Spain and the Peruvian University of Applied Sciences (UPC). She is currently studying for a Master's of Business Administration (MBA) at the UPC. Fátima has extensive experience in International Trade Law, Regional and Multilateral Integration, and New Technologies Law. She has served as an international official in the General Secretariat of the Andean Community, first in the Legal Service, then as coordinator of the Services, Transportation, Intellectual Property, Investments and Public Procurement Programs. In addition, for three years, she assumed the position of Secretariat of the Commission of the Andean Community, the decision-making body in matters of trade and investment of said international organisation. Fátima is also a tutor on virtual courses on Electronic Government organised by the Organization of American States (OAS) and a consultant for Alfa-Redi for the Project "Digital Files in the Commercial Courts of Lima".

**Iriarte & Asociados**
Calle Enrique Palacios N° 360, office. 612
Miraflores
Lima
Peru

Tel: +51 99 797 6780
Email: ftoche@iriartelaw.com
URL: www.iriartelaw.com

Iriarte & Asociados is a group of lawyers specialised in the interrelationship between Law and the Information Society, with the policy areas and regulatory framework of the Information Society being our main strength, together with the so-called law of new technologies and intellectual property, including data protection.

Our legal practice is constantly fed with academic work and scientific activity, as well as policy consulting, which allows us to understand in greater depth the new changes that information and communication technologies pose in society, and in this way to be able to provide the services that your company or organisation requires to face the new challenges required by the Information Society.

The correct understanding and knowledge of the new information and communication technologies, added to our experience in technological businesses and the use of intellectual property as a tool for the protection and enhancement of our clients' companies are some of our main strengths: therefore, we are able to provide you with a wide range of strategies for the registration, maintenance, use and protection of your intangible capital, intellectual and industrial property, as well as facing the challenges of the Information Society in strict respect of current legislation.

But we have not only taken New Technologies as the north, the Material and Intangible Cultural Heritage, as a human creation that must be respected; as well as the Environment, which is where the human being develops, are part of our specialisations, achieving together with Intellectual Property, Cultural and Creative Industries and the Law of New Technologies an amalgam of modernity and respect for our historical legacy; of new digital technologies and recognition of the inventive capacity and sensitivity of the human being through creation and art. We are a mixture of our past and our future living in the present.

**www.iriartelaw.com**

# Poland


Grzegorz Leśniewski


Mateusz Borkiewicz


Jacek Cieśliński

Leśniewski Borkiewicz & Partners

## 1 Relevant Legislation and Competent Authorities

### 1.1 What is the principal data protection legislation?

Since 25 May 2018, the principal data protection legislation in Poland has been Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation) ("GDPR").

### 1.2 Is there any other general legislation that impacts data protection?

Yes, there is further general legislation that impacts data protection. The key laws are:

1. **Protection of Personal Data Act of 10 May 2018**.
   This specifies in particular:
   a. the procedure for notifying the appointment of a Data Protection Officer ("DPO");
   b. the conditions of accreditation of the entity authorised to certify in the field of personal data protection;
   c. the procedure for approving codes of conduct;
   d. monitoring compliance with the personal data protection provisions; and
   e. criminal liability for violating such provisions.
2. **The Telecommunications Act of 16 July 2004 (ePrivacy Directive implementation, revised by Directive 2009/136). In practice, this applies to every entrepreneur with a website**.
   Article 173 of the Telecommunications Act is a general provision and applies to every entity that uses technology such as cookies, regardless of the nature of the data being stored or accessed.
   It sets a specific standard for all entities (regardless of the sector – online, mobile, e-commerce, other information society services ("ISS"), connected vehicles, etc.) that wish to store or access information stored not only on computers, but in all terminal equipment (smartphones, smart TVs, etc.).
   The obligation to meet additional requirements applies largely to commonly used solutions, starting from collecting information for statistical purposes or behavioural marketing (client profiles), through anti-fraud tools used by website operators (e.g. for 'clickbot' detection), to building an online advertising network.
3. **Labour Code of 23 December 1997**.
   This regulates, among others, the scope of data that the employer may request from the employee or the right to monitor employees.
4. **Protection of Personal Data Processed in Connection with Preventing and Combating Crime Act of 14 December 2018 (Police Directive implementation)**.
   This regulates the area excluded from the application of the GDPR, i.e. the processing of personal data by competent authorities for the purposes of crime prevention, conducting preparatory proceedings and detecting offences.
5. **Articles 101 and 102 of the Treaty on the Functioning of the EU (regarding the definition of the term 'undertaking')**.
   According to recital 150 of the GDPR, where administrative fines are imposed on an 'undertaking', an 'undertaking' should be understood in accordance with Articles 101 and 102 TFEU for those purposes (which unfortunately may have an adverse effect on the amount of the fine from the entrepreneur's perspective).

### 1.3 Is there any sector-specific legislation that impacts data protection?

Yes. Specifying the provisions of the GDPR is a typical occurrence in the Polish legal system for most sectors.

The key sectoral legislation in Poland includes (the following list is not exhaustive):

1. Provision of Electronic Services Act of 18 July 2002 – regulating areas such as ISS (e-commerce, hosting, etc.);
2. National Cybersecurity System Act of 5 July 2018 – regulating, *i.a.*, the required level of network and IT systems security of key service operators and digital service providers (online trading platforms, cloud computing services, Internet search engines);
3. Banking Act of 29 August 1997;
4. Payment Services Act of 19 August 2011;
5. Insurance and Reinsurance Activity Act of 11 September 2015;

6. Counteracting Money Laundering and Terrorist Financing Act of 1 March 2018;
7. Medical Activities Act of 15 April 2011; and
8. Energy Law Act of 10 April 1997.

### 1.4 What authority(ies) are responsible for data protection?

As a rule, the authority responsible for the protection of personal data in Poland is the President of the Personal Data Protection Office (as a supervisory authority within the meaning of the GDPR).

In some cases of processing with a cross-border element, the competent authority to take action concerning data protection may be the supervisory authority of another EU Member State (acting as the lead supervisory authority).

## 2 Definitions

### 2.1 Please provide the key definitions used in the relevant legislation:

- "**Personal Data**"
  Any information concerning an identified or identifiable natural person.
  To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, either by the controller or by another person, to identify the natural person directly or indirectly. When assessing whether the means are of this nature, all objective factors should be taken into consideration – costs, time, technology, etc.
  Examples of personal data include: name; identification number; location data; online identifier, such as an IP address; ID cookie (especially when combined with marketing data); and other factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a natural person.
- "**Processing**"
  Any operation or set of operations which is performed on personal data, whether or not by automated means.
  In other words, "processing" means any action taken on personal data during "the lifetime of the information" – including the collection of personal data (initial stage) and their deletion (last stage). Any other operations, such as profiling or pseudonymisation, shall also be considered as "processing".
- "**Controller**"
  The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
  The GDPR establishes the responsibility and liability of the controller for any processing of personal data carried out on the controller's behalf.
- "**Processor**"
  A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
- "**Data Subject**"
  An identified or identifiable natural person; an individual who is the subject of the relevant personal data – in other words, any person whose personal data are being processed.
  The protection afforded by the GDPR applies to natural persons, whatever their nationality or place of residence.
  The GDPR does not cover the processing of personal data which concern legal persons, including the name, form and contact details.
- "**Sensitive Personal Data**"
  Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data (if processing for the purpose of uniquely identifying a natural person), data concerning health or a natural person's sex life or sexual orientation (closed catalogue).
  The processing of Sensitive Personal Data requires the fulfilment of additional obligations, including in the field of data security (there are further technical and organisational measures to take and, in most cases, a need to carry out a Data Protection Impact Assessment – "DPIA").
- "**Data Breach**"
  A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
- "**Profiling**"
  Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
- "**Pseudonymisation**"
  The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

## 3 Territorial Scope

### 3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

Regardless of whether or not the processing takes place in the EU, the GDPR applies to businesses that are established in any EU Member State and that process personal data (either as a controller or processor) in the context of that establishment.

**Businesses established in another jurisdiction**

The GDPR applies to businesses established outside the EU if they process the personal data of EU residents in relation to the: (i) offering of goods or services (whether or not in return for payment) to EU residents; or (ii) monitoring (including tracking on the Internet) of the behaviour of EU residents (to the extent that such behaviour takes place in the EU).

In such cases, they are obligated to designate a representative in the EU (a natural or legal person established in the EU who represents them with regard to their respective obligations under the GDPR).

## 4 Key Principles

### 4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  Personal data must be processed lawfully, fairly and in a transparent manner. Controllers must provide certain minimum information to data subjects regarding the collection and further processing of their personal data. Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
  When collecting personal data via the Internet, including mobile devices, providing information in a multi-layered manner is good practice (in some cases, it may even be considered an obligation).
- **Lawful basis for processing**
  The GDPR provides an exhaustive list of legal bases for processing. The following are the most relevant for businesses: (i) consent of the data subject; (ii) contractual necessity; (iii) compliance with legal obligations; or (iv) legitimate interests (pursued by the controller or by a third party), except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.
  The GDPR requires stronger grounds to process sensitive personal data (compared to "regular" personal data; there is no possibility to rely on the contract or legitimate interest).
- **Purpose limitation**
  Personal data may only be collected for specified, explicit and legitimate purposes, and must not be further processed in a manner that is incompatible with those purposes. If a controller wishes to use the relevant personal data in a manner that is incompatible with the purposes for which they were initially collected, it must: (i) inform the data subject of such new processing; and (ii) be able to rely on a lawful basis as set out above.
  Having a legal basis for processing for a specific purpose does not mean the possibility of using all potentially valuable personal data for its implementation (which data may be collected for a specific purpose is determined by the principle of minimisation, as set out below).
- **Data minimisation**
  Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed.
- **Proportionality**
  The need to maintain appropriate proportions of the scope of data for the purposes of processing and to process only such data that are necessary for the implementation of specific purposes.
- **Retention**
  Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
  It is good practice (sometimes even an obligation resulting from the accountability requirement) to implement internal data review procedures to determine the maximum storage period.
- "**Accountability**"
  The controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.
  In the case of automated processing, this means, in particular, the need to ensure that relevant information is recorded in IT system logs.
- "**Data security (integrity and confidentiality)**"
  Personal data must be processed in a manner that ensures appropriate security of those data, including protection against unauthorised or unlawful processing and against accidental loss, using appropriate technical or organisational measures.
  The provisions do not specify measures to be implemented (due to the technological and organisational neutrality of the GDPR). The burden of choosing each specified measure to ensure data security lies with the controllers. Such an approach causes uncertainty, but also allows controllers to focus on areas where data processing can result in a "high risk" (for privacy). Far-reaching safeguards will not always be needed in cases of "low risk" processing.
- "**Accuracy**"
  Personal data must be accurate and, where necessary, kept up to date. A business must take every reasonable step to ensure that personal data that are inaccurate are either erased or rectified without delay.

## 5 Individual Rights

### 5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**
  The data subject has the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data.
  The data subject has also the right to obtain from a controller information on processing, in particular about: (i) the purposes of the processing; (ii) the categories of data being processed; and (iii) where the data were not collected from the data subject, information as to the source of the data.
  The data subject may also request a copy of the personal data being processed. Such copy may take the form of, in particular, a photocopy of the document or a copy of the printout from the IT system (it should therefore be designed to enable such an operation).
- **Right to rectification of errors**
  Controllers must ensure that inaccurate or incomplete data are erased or rectified (the data subject has the right to request such actions).
- **Right to deletion/right to be forgotten**
  Where the controller has made the personal data public and is obliged (pursuant to the above point) to erase the personal data, the controller has to take reasonable steps to inform other controllers that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those data.

- **Right to object to processing**
  Data subjects have the right to object, on grounds relating to their particular situation, to the processing of personal data where the basis for that processing is either public interest or legitimate interest.
  The controller must cease such processing unless it demonstrates compelling legitimate grounds for the processing which overrides the interests, rights and freedoms of the relevant data subject or requires the data in order to establish, exercise or defend legal rights.
  If the data subject objects to processing for a direct marketing purpose (including profiling), raising an objection means that the data cannot be further processed for such purpose.
  The right to object applies only to data processing on the above legal grounds (public interest or legitimate interest).
- **Right to restrict processing**
  Data subjects have the right to restrict the processing of personal data, which means that the data may only be held by the controller and may only be used for limited purposes. It applies if, *i.a.*: (i) the accuracy of the data is contested; (ii) the processing is unlawful and the data subject requests restriction (as opposed to exercising the right to erasure); or (iii) verification of overriding grounds is pending, in the context of an objection to processing.
- **Right to data portability**
  The data subject is allowed to receive personal data concerning him or her in a structured, commonly used, machine-readable and interoperable format. Where technically feasible, the data subject has the right to have the personal data transmitted directly from one controller to another (also conducting competitive activity). This does not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible.
  The data subject's right to transmit or to receive data applies only:
  - to data provided to a controller by a data subject. The data observed by the controller is also considered to be such – e.g., in the online environment, it could be data regarding the tracked activity of the data subject on the website. Such data does not include data "created" by the controller as a result of profiling (e.g. "the customer is interested in premium products");
  - where the processing of personal data is carried out by automated means (as a consequence, IT systems should be designed to enable the export of data of a specific person); or
  - where processing is based on consent or contract. It does not apply where processing is based on other legal grounds.
- **Right to withdraw consent**
  When processing of personal data is based on consent of the data subject, the data subject has a right to withdraw the consent given at any time. In such case, in the absence of the other legal basis for further processing of personal data of the data subject, the controller needs to erase personal data.
  Withdrawal of the consent given does not affect the lawfulness of processing based on consent before its withdrawal.
- **Right to object to marketing**
  At any time a data subject may object without cause to the processing for the purposes of direct marketing. Should such objection be submitted, the data controller will not be allowed to process personal data for the data subject for that purpose.
- **Right to complain to the relevant data protection authority(ies)**
  The data subject is entitled to lodge a complaint to the supervisory authority; in Poland it is the President of the Personal Data Protection Office. A detailed description of the complaint procedure is available at: https://uodo.gov.pl/pl/83/155.
- **Right to erasure**
  If the controller does not have the basis for further processing, the data subject has the right to obtain from the controller the erasure of personal data. This applies when (*i.a.*): the data subject withdraws consent or exercises the right to object, which turns out to be effective.
  Where the controller has no basis for further processing, he needs to erase personal data even in the absence of such a request from the data subject.

## 6 Registration Formalities and Prior Approval

### 6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

The controller is required to report and consult the supervisory authority when, after conducting a DPIA, it appears that it creates a high risk of violation of rights and freedoms, and the controller cannot implement sufficient measures to reduce such risk to an acceptable level.

For information regarding notification of a DPO, please see question 7.7.

For information regarding the reporting of data breaches, please see section 15.

### 6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

The notification concerns particular types of processing and must be fairly specific.

### 6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

Registrations/notifications are made according to the type of processing.

### 6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

Registration/notification is required for any controller who is subject to the GDPR and intends to start a processing operation meeting the notification obligation.

### 6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

The notification should include:

- the identity and the contact details of the controller;
- the respective responsibilities of the controller, joint controllers and processors involved in the processing;
- the purposes and means of the intended processing;
- the measures and safeguards provided;
- the contact details of the DPO;
- the DPIA; and
- any other information requested by the supervisory authority.

### 6.6 What are the sanctions for failure to register/notify where required?

Failure to comply with such obligation may result in the imposition of an administrative fine of up to EUR 10,000,000 or, in the case of an undertaking, up to 2% of the total worldwide annual turnover.

The authority may also exercise corrective powers (described in section 16).

### 6.7 What is the fee per registration/notification (if applicable)?

Registration/notification is free of charge.

### 6.8 How frequently must registrations/notifications be renewed (if applicable)?

Whenever the risk resulting from processing changes, the controller reviews it to determine whether the processing is carried out in accordance with the DPIA and whether there is a need for re-consultation.

### 6.9 Is any prior approval required from the data protection regulator?

In the abovementioned case, the controller can start processing only after obtaining confirmation that such operation is GDPR-compliant.

### 6.10 Can the registration/notification be completed online?

An electronic form for prior consultation is available. To use this form, an account on the ePUAP platform is needed. It can be created, *i.a.*, through the website: https://epuap.gov.pl.

### 6.11 Is there a publicly available list of completed registrations/notifications?

No such list is available.

### 6.12 How long does a typical registration/notification process take?

The supervisory authority should review the application within eight weeks. Due to the complex nature of the intended processing, the authority may extend the period by an additional six weeks.

## 7 Appointment of a Data Protection Officer

### 7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

The appointment of a DPO for controllers or processors is only mandatory in some circumstances, including where there is: (i) large-scale regular and systematic monitoring of individuals, e.g. on the Internet (as a core activity); or (ii) large-scale processing of sensitive personal data and personal data relating to criminal convictions and offences (as a core activity).

### 7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

In the circumstances where appointment of a DPO is mandatory, failure to comply may result in imposing an administrative fine of up to EUR 10,000,000 or, in the case of an undertaking, up to 2% of the total worldwide annual turnover.

### 7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

The appointed DPOs should not be dismissed or penalised for performing their tasks and should report directly to the highest management level of the controller or processor.

### 7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

A single DPO is permitted for a group of undertakings, provided that the DPO is easily accessible from each establishment.

### 7.5 Please describe any specific qualifications for the Data Protection Officer required by law.

The DPO should be appointed on the basis of professional qualities and should have expert knowledge of data protection law and practices. While this is not strictly defined, it is clear that the level of expertise required depends on the circumstances. For example, the involvement of large volumes of sensitive personal data will require a higher level of knowledge.

### 7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

A DPO should be involved in all issues which relate to the protection of personal data. The GDPR outlines the minimum tasks

required by the DPO, which include: (i) monitoring compliance with the GDPR, national legislation and internal policies; (ii) advising on DPIA and the training of staff; and (iii) acting as the authority's primary contact point.

**7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?**

The President of the Personal Data Protection Office must be notified of the DPO's appointment within 14 days from the date of designation.

**7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?**

The DPO's data (first name, surname and email address or telephone number) must be available on the controller's or processor's website.

The data subject must be notified only of the contact details of the DPO when personal data are collected.

## 8 Appointment of Processors

**8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?**

Yes. The business that appoints a processor to process personal data on its behalf, is required to enter into an agreement with the processor which sets out, in particular, the subject matter for processing, the duration of processing, the nature and purpose of processing, the types of personal data and the categories of data subjects.

It is essential that the processor appointed by the business complies with the GDPR.

**8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?**

The processor must be appointed under a binding agreement in writing (including in electronic form). The contractual terms must stipulate that the processor, *i.a.*: (i) only acts on the documented instructions of the controller; (ii) imposes confidentiality obligations on relevant entities; (iii) ensures the security of personal data that it processes; and (iv) abides by the rules regarding the appointment of sub-processors.

## 9 Marketing

**9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).**

Sending commercial information (intended directly or indirectly to promote the goods, services or image of the entrepreneur) to a designated recipient by means of electronic communication (via email, SMS, webpush, Messenger, WhatsApp, etc.) requires his/her consent ("opt-in" system).

The consent must be GDPR-compliant (*i.a.*, separate for each communication channel) – consent may be expressed by providing an electronic address (e.g. email).

There are practical doubts concerning the possibility of sending electronic requests for such consent. The courts' and authorities' approach is not consistent.

Regardless of these requirements, the phone number, email address, etc. constitute personal data within the meaning of the GDPR. An entity operating in the field of electronic marketing must also provide a legal basis for data processing for this purpose (usually it will be a legitimate interest or contract – e.g. the provision of a newsletter service).

**9.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?**

The obligation to obtain consent applies to sending commercial information to natural and also legal persons (although there are some doubts in this respect).

**9.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).**

**Marketing *i.a.* by telephone**

The use of telecommunications terminal equipment and automated calling systems for direct marketing purposes requires consent ("opt-in" system). The consent must be GDPR-compliant.

This means that telephone contact for marketing purposes also requires the prior approval of the recipient of such activities. This requirement applies to activities targeted at each entity (B2C and B2B, regardless of whether it is a natural or legal person). In the case of natural persons, however, the telephone number will also constitute personal data (regardless of the aforementioned requirements – the telephone marketing entity must also provide a legal basis for data processing for this purpose).

**Marketing by post (targeted at a specific entity)**

Although such actions do not have to meet additional requirements such as in the case of electronic or telephone marketing, it is necessary to meet the requirements of the GDPR.

This means the need to provide a legal basis for such action (generally, it will be a legitimate interest resulting from the seller–customer relationship). However, it cannot be ruled out that in some cases – especially when there is no such relationship between the controller and the data subject – it will be necessary to have consent in order to conduct marketing by post.

**9.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?**

Yes, the requirements apply to marketing activities conducted by European and other international senders, when targeting entities based/resident in Poland.

### 9.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

Yes. The penalty imposed in regard to electronic marketing activities was about PLN 201,000 – for an ineffective system of withdrawal of the consent for data processing (Polish supervisory authority).

Marketing activities undertaken in Poland without the required consent may also constitute a practice that violates the collective interests of consumers (in accordance with the Competition and Consumer Protection Act).

Therefore, the Office for Competition and Consumer Protection shows the greatest activity in enforcing infringements by telemarketers – including by imposing financial penalties (the maximum amount may be up to 10% of turnover; it is also possible to impose sanctions directly for persons in the company's governing bodies – up to PLN 2 million).

### 9.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

The purchase of marketing lists must meet the requirements of the GDPR; in particular:

- There must be a legal basis for the transfer of such data. Depending on the case, this may be: a contract – e.g. the appropriate arrangement of a loyalty programme; legitimate interest – recital 47 allows the legitimate interest of the data collector (the list buyer) to be referred to. Mostly, however, this will mean the need to have consent from the data subject.
- The data subject should be informed about such a transfer (in particular, about the source of the data acquisition by the buyer and its scope).

It cannot be ruled out that the purchase of such a database will also have to meet the requirements of the Protection of Databases Act (*i.a.*, the purchase from the relevant entity – "database producer").

In order for the marketing base to fulfil its economic purpose (enabling the buyer to continue using it for marketing purposes), the buyer should have his/her own legal basis for such activities.

The following best practices are recommended:

- the person receiving the marketing message should know who is sending the message (the information as part of the message), and on whose behalf; and
- marketing activities should be based on a contract that includes a mechanism for transferring rights and obligations from such a contract to a third party.

### 9.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

In case of a violation of the GDPR (no legal basis/failure to comply with the information obligation), there is a penalty of up to EUR 20,000,000, and in the case of an enterprise, up to 4% of its total annual global turnover.

Lack of consent mentioned in questions 9.1 and 9.3 may result in:

- a penalty of up to 3% of income (for violation of the Telecommunications Act); or
- a penalty of up to 10% of turnover (if the actions are considered to be practices violating collective consumer interests; with a possible penalty of up to PLN 2 million for persons in the company's governing bodies).

## 10 Cookies

### 10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

As a rule, prior consent is required for cookies (or similar technologies). This applies, in particular, to the use of cookies in devices such as a computer, smartphone or smart TV.

### 10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

Provisions allow the use of some cookies to be exempted from the requirement of informed consent. This applies to cookies that meet one of the following criteria:

- the cookie is for the sole purpose of carrying out the transmission of a communication over an electronic communications network; or
- the cookie is strictly necessary to provide an "information society service" requested by the subscriber or user, which means that it must be essential to the fulfilment of their request.

### 10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

The Polish data protection authority has not yet taken any enforcement action in relation to cookies.

### 10.4 What are the maximum penalties for breaches of applicable cookie restrictions?

Violation of the requirements for the use of cookies entails a possible penalty of up to 3% of revenue (Telecommunications Act).

An incorrect cookie mechanism may also constitute a violation of the GDPR (no legal basis for processing) and, as a consequence, a penalty within the limits provided for by the data protection provisions.

## 11 Restrictions on International Data Transfers

### 11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

Data transfers to other jurisdictions that are not within the European Economic Area can only take place if: (i) the transfer is to a territory/country which ensures an adequate level of protection (as specified by the EU Commission, *i.a.* to Japan and Switzerland); (ii) the business has implemented one of the required safeguards as specified by the GDPR (described below); or (iii) one of the derogations specified in the GDPR applies to the relevant transfer (e.g. data subject consent).

**11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).**

For international transfers of personal data (to a country which does not ensure an adequate level of protection), common options are:

- the use of Standard Contractual Clauses (drafted by the EU Commission); and
- for international data transfers within a group of businesses – the implementation of Binding Corporate Rules ("BCRs") (which, however, require approval from the relevant data protection authority).

**11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.**

Some of the safeguards outlined in the GDPR that legalise international data transfers will require prior approval from the relevant data protection authority, including the establishment of BCRs or a code of conduct (also legalising such data transfer).

The time required to obtain such approval depends on the case.

**11.4 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?**

The Polish data protection authority has not issued any guidelines following the decision of the Court of Justice of the EU in *Schrems II*. The approach of the Personal Data Protection Office is to rely on guidelines drawn by the EDPB.

Until the date of this study, the EDPB adopted recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, as well as recommendations on the European Essential Guarantees for surveillance measures.

Both documents were adopted as a follow-up to the CJEU's '*Schrems II*' decision. The recommendations on the supplementary measures are to help controllers and processors acting as data exporters with identifying and implementing appropriate supplementary measures where they are needed to ensure an essentially equivalent level of protection to the data they transfer to third countries.

The recommendations on the supplementary measures were submitted to public consultation which ended on 21 December 2020, and they are still subject to possible further modifications on the basis of the results of the public consultation.

The recommendations on the European Essential Guarantees are complementary to the recommendations on supplementary measures and provide data exporters with elements to determine if the legal framework governing public authorities' access to data for surveillance purposes in third countries can be regarded as not impinging on the provisions of Article 46 GDPR.

**11.5 What guidance (if any) has/have the data protection authority(ies) issued in relation to the European Commission's revised Standard Contractual Clauses?**

No separate guidance has been issued by Polish data protection authority. The President of the Personal Data Protection Office decided that his position on the draft would be prepared jointly with other members of the European Data Protection Board.

On 14 January 2021 the EDPB and EDPS adopted joint opinions on two sets of standard contractual clauses ("SCCs"): one opinion on the SCCs for contracts between controllers and processors and one on the SCCs for the transfer of personal data to third countries.

In general, the opinions that concluded the draft SCCs present a reinforced level of protection for data subjects. Nevertheless, the EDPB and EDPS stated that several provisions could be improved or clarified, as for example: the scope of the SCCs; certain third-party beneficiary rights; certain obligations regarding onward transfers; aspects of the assessment of third country laws regarding access to public data by public authorities; and the notification to the supervisory authority.

## 12 Whistle-blower Hotlines

**12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?**

**Current scope**

Internal whistle-blowing schemes are generally established in pursuance of a concern to implement proper corporate governance principles in the daily functioning of businesses.

The scope of corporate whistle-blower hotlines does not need to be limited to any particular issue. It is recommended that the business responsible for the whistle-blowing scheme should carefully assess whether it might be appropriate to limit the number of persons eligible for reporting alleged misconduct; in particular, in the light of the seriousness of the alleged offences reported.

**From 2021 (after the implementation of the Directive on the protection of persons reporting on breaches of Union law which shall happen by 17 December 2021)**

The Whistleblower Directive protects persons reporting on breaches.

New regulations include an obligation to:

- implement internal channel reporting procedures; and
- share information with both employees and business partners regarding the possibility of reporting on breaches, including through external channels, to the competent authorities.

**12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?**

The Whistleblower Directive does not explicitly require that channels for reporting on breaches ensure anonymity.

However, the provisions specify that disclosure of the identity of the reporting person should be allowed where the disclosure of data is a necessary and proportionate obligation required

under EU or national law in the context of investigations or subsequent judicial proceedings, or to safeguard the freedoms of others, including the right of defence of the concerned person. Apart from these cases, the identity of the whistle-blower is to be protected.

## 13 CCTV

**13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?**

**Notification**
The obligation to notify the authority before the implementation of CCTV may occur in the cases described in section 6, as a consequence of the DPIA. This must be undertaken for, e.g. (but not limited to), systematic monitoring of a publicly accessible area on a large scale.

**Form of public notice**
The controller should inform data subjects who could potentially be monitored: (i) that monitoring is used; (ii) what area is covered by it; and (iii) its purpose and other information included in Article 13 GDPR.

Data subjects who remain in the monitored area must be aware that monitoring is carried out. Notices informing of the monitoring installed should be visible and placed permanently, not too far away from the monitored places.

It is not sufficient to mark the area covered by monitoring only with pictograms (they can be used additionally), as the information obligation specified in Article 13 GDPR should also be met. This does not mean that all information indicated in this provision should be provided at once. It is permitted to use layered information notices.

**13.2 Are there limits on the purposes for which CCTV data may be used?**

The provisions do not limit the purposes for which CCTV can be used (with the exception of special regulations regarding, *i.a.*, employer monitoring; restrictions introduced by sector-specific legislation, e.g. educational legislation or that which regulates public monitoring applied by local government units, are also possible).

General limitations of the CCTV purposes may result from the principle of proportionality, especially in the case of combining CCTV with other solutions, such as facial recognition.

The controller must also provide a legal basis for the use of CCTV – and although all the grounds under Article 6 GDPR are available, in individual cases it may be difficult to find a suitable one for a specific purpose other than compliance with a legal obligation or resulting from a legitimate interest of the controller (e.g. security of persons or property).

## 14 Employee Monitoring

**14.1 What types of employee monitoring are permitted (if any), and in what circumstances?**

**CCTV**
The employer may introduce monitoring (of the workplace or area around it) only if it is necessary to: (i) ensure employee safety or property protection; (ii) ensure production control; or (iii) keep the information confidential, the disclosure of which could expose the employer to harm.

CCTV may not cover certain rooms (e.g. sanitary areas).

**Email monitoring**
The employer may introduce control of an employee's official email only if it is necessary to ensure: (i) the organisation of work (full use of working time); and (ii) proper use of the work tools provided to the employee.

Such monitoring cannot violate the confidentiality of correspondence or other personal rights of the employee.

**Other forms of monitoring**
The employer may implement other forms of monitoring (e.g. online computer use, geolocation monitoring) if their use is necessary to achieve purposes corresponding to email monitoring (e.g. organisation of working time, proper use of work tools).

Such solutions must, however, always meet the other requirements of the GDPR, including adequacy for the purposes of processing.

**14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.**

The employer should inform employees about the implementation of monitoring, in the manner adopted by the employer (e.g. via intranet), no later than two weeks before its launch.

Also, before allowing a new employee to work, the employer should provide him/her with information about monitoring in writing.

**14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?**

The purpose, scope and method of application of monitoring should be set out in the corporate collective labour agreement or in the work regulations (unless the employer is not obliged to implement these documents – usually when employing less than 50 employees).

As a rule, this means that the employer must agree on the use of monitoring with the trade union organisation if one operates at a company.

## 15 Data Security and Data Breach

**15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?**

Yes. The controller and the processor must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk (such actions may include, *i.a.*, the pseudonymisation and encryption of personal data).

The GDPR does not specify measures to be implemented (technological and organisational neutrality of the GDPR). The burden of choosing each specified measure to ensure data security lies with the controller and the processor.

**Responsibility**

As a rule, the GDPR establishes the responsibility of the controller for any processing of personal data carried out on the controller's behalf. This also applies to operations undertaken by the processor (this does not, of course, exclude the processor's contractual liability; nonetheless, if the processor infringes the GDPR by determining the purposes and means of processing, it will take responsibility as a controller in respect of that processing).

**15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

The controller is responsible for reporting a personal data breach without undue delay (and in any case within 72 hours of becoming aware of the breach – after this term, it needs to be accompanied by reasons for the delay) to the relevant data protection authority, unless the breach is unlikely to result in a risk to the rights and freedoms of the data subject(s).

The notification must include, *i.a.*: the nature of the data breach, including the categories and number of data subjects concerned, the likely consequences of the breach and the measures taken to address the breach, including attempts to mitigate possible adverse effects.

**15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

Controllers have a legal requirement to communicate the data breach to the data subject, without undue delay, if it is likely to result in a high risk to the rights and freedoms of the data subject.

The notification must include, *i.a.*, the likely consequences of the breach and any measures taken to remedy or mitigate the breach.

The controller may be exempt from notifying the data subject, if he/she has taken measures to minimise the risk of harm (e.g. suspending affected accounts) or the notification requires a disproportionate effort (in such a case, there shall instead be a public communication or similar measure).

**15.4 What are the maximum penalties for data security breaches?**

The maximum penalty is EUR 10 million or 2% of worldwide annual turnover.

## 16 Enforcement and Sanctions

**16.1 Describe the enforcement powers of the data protection authority(ies).**

(a) **Investigative Powers**: power to order the controller and the processor to provide any information it requires for the performance of its tasks or to conduct investigations in the form of data protection audits.

(b) **Corrective Powers**: power to issue warnings for non-compliance or to impose a permanent or temporary ban on processing.

(c) **Authorisation and Advisory Powers**: power to authorise codes of conduct, give opinions on assumptions or drafts of the legal acts concerning personal data processing, authorise binding corporate rules and grant relevant authorisations; power to issue guidelines in matters related to processing of personal data.

(d) **Imposition of administrative fines for infringements of specified GDPR provisions**: power to impose fines of up to EUR 20 million or 4% of the business' worldwide annual turnover.

(e) **Non-compliance with a data protection authority**: the data protection authority may also impose fines in the course of administrative proceedings, for example for failure to provide information required by the President of Personal Data Protection Office or for providing insufficient information.

**16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?**

The GDPR entitles data protection authorities to impose a temporary or definitive limitation, including a ban on processing. Such a ban does not require a court order.

**16.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.**

According to information made available by the Polish supervisory authority on its website, in 2020 it issued nine decisions imposing administrative fines in a total amount of approx. PLN 3,195,588 million (approx. EUR 702,327). In seven cases, penalties were imposed on private sector entities; and in two, on public entities.

In the remaining scope, the authority either exercised corrective powers (primarily by imposing a ban on further processing or an order to adapt it to the requirements) or discontinued the proceedings.

At the time of writing this information, according to information made available by the Polish supervisory authority on its website, in 2021 it issued six decisions imposing administrative fines of a total amount of approx. PLN 379,000. In four cases, penalties were imposed on private sector entities; in two, on public entities.

**16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?**

At the time of writing, the Personal Data Protection Office ("UODO") informed that the office had sent a request to the Lithuanian supervisory authority for assistance regarding Vinted UAB with its seat in Lithuania. The reason for sending a request is a practice adopted by the company requiring users of vinted website/ application to present copies of their identity cards.

The Office – under the mutual cooperation mechanism – submitted a request pursuant to Art. 61 GDPR to the State Data Protection Inspectorate (Lithuanian supervisory authority) to initiate *ex officio* proceedings or to conduct an inspection at Vinted UAB in order to adapt the processing operations to the provisions of the GDPR.

## 17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

### 17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Most businesses weigh the risk of non-compliance with the relevant foreign court/authority order against the risk of non-compliance with the data protection regulations, and determine which one is lower. Any data transfer in response to a foreign request must be compliant with provisions on international data transfer.

When disclosing the requested personal data, businesses usually seek to justify such actions on the basis of necessity for the establishment, exercise or defence of legal claims.

### 17.2 What guidance has/have the data protection authority(ies) issued?

Guidance at the international level is relevant in this area.

Article 29 Data Protection Working Party (currently replaced by the European Data Protection Board) adopted on 11 February 2009 is the Working Document on pre-trial discovery for cross-border civil litigation.

The European Data Protection Board adopted on 25 May 2018 establishes the Guidelines on derogations of Article 49 under the GDPR (these also raise the topic of data transfers for the purpose of formal pre-trial discovery procedures).

## 18 Trends and Developments

### 18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

Proceedings carried out so far ended with the imposition of penalties which showed the approach to administrative fines adopted by the Polish supervisory authority (in line with the European trend) – a significant emphasis on the dissuasive function of the penalty. Its amount is not only to deter the addressee from repeated violations, but also to effectively discourage other entities from violating the rules of personal data protection in the future.

Few penalties were imposed for the lack of data breaches notification and for lack of cooperation with the Polish supervisory authority during proceedings. Two top penalties imposed in 2020 amounted to:

- PLN 1,000,000 – for not implementing appropriate technical and organisational measures which led to a loss of confidentiality of personal data; and
- PLN 1,900,000 – for lack of appropriate technical and organisational measures to ensure the security of the processed data.

### 18.2 What "hot topics" are currently a focus for the data protection regulator?

Poland fits into broader international trends.

1. Increased work can be observed primarily in the area of regulating new technological solutions using personal data. In particular (at European level):
   - in February 2020, the European Commission issued the White Paper for Artificial Intelligence (announcement of legal changes in the area of AI);
   - in January 2020, the EDPB completed a public consultation on the guidelines to the implementation of the principles of privacy by design and by default (key for the IT industry, among other sectors);
   - in 2019, the European Commission published the Report 'Liability For AI and Other Emerging Digital Technologies'; and
   - the guidelines on processing personal data in the context of connected vehicles and mobility-related applications are also being developed.
2. As a result of decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18):
   - in December 2020, the EDPB completed a list of public consultations on guidelines on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data; and
   - 14 January 2021 the EDPB and EDPS adopted joint opinions on two sets of SCCs: one opinion on the SCCs for contracts between controllers and processors and one on the SCCs for the transfer of personal data to third countries.
3. Also due to the COVID-19 pandemic the data protection regulator focuses also on such aspects of processing personal data as:
   - processing the personal data of special categories, *i.a.*, by entrepreneurs, including employees;
   - processing personal data by educational sector in the light of remote schooling;
   - processing of personal data in the light of remote working (safe use of videocalls, admissibility of processing personal data stored on a paper by remote employees, etc.);
   - apps supporting the prevention of COVID-19; and
   - incidents related to disclosure of personal data of quarantined persons.

**Grzegorz Leśniewski** has been advising since 2009. His main areas of practice include personal data protection, new technologies law, cybersecurity and M&A.
For six years, he worked at one of the major law firms in Poland, where for the last two years he managed the company's Warsaw office and was responsible for the TMT and M&A areas of specialisation. Later he developed the boutique law firm Leśniewski Legal, under which he advised on, among other matters, the implementation of the GDPR by a Norwegian global provider of telecommunications and cable television services. He has also been the Data Protection Officer at one of the major cloud computing companies in Poland since the entry into force of the GDPR.
Grzegorz has managed the implementation of numerous M&A processes, as well as negotiations in the process of buying/selling companies, mostly in the TMT sector.
He is also on the list of attorneys kept by the District Bar Council in Warsaw, Poland.

**Leśniewski Borkiewicz & Partners**
ul. Podwale 83 / 11
50-414 Wrocław
Poland

Tel: +48 531 871 707
Email: gl@lbplegal.com
URL: www.lbplegal.com/en

**Mateusz Borkiewicz** has been advising since 2010. He was an associate at one of the major law firms in Poland for almost five years, where he also held a managerial position with primary responsibility for the practices regarding the GDPR and TMT industries in general.
He has advised on strategic topics concerning, among others, issues of unfair competition, protection of trademarks, cybersecurity, domain disputes, spam, violations of personal rights on the Internet (particularly in the context of hate speech towards public figures), managerial bribery and computer crimes, including virtual currencies theft. At the same time, he has been involved in *pro bono* projects in cooperation with the Helsinki Foundation for Human Rights.
Mateusz has served as a Data Security Administrator and Data Protection Officer in several companies operating in the financial services, retail and automotive sectors.
He is also on the list of attorneys kept by the District Bar Council in Wrocław, Poland.

**Leśniewski Borkiewicz & Partners**
ul. Podwale 83 / 11
50-414 Wrocław
Poland

Tel: +48 663 683 888
Email: mb@lbplegal.com
URL: www.lbplegal.com/en

**Jacek Cieśliński** has been advising since 2015. His counselling includes ongoing assistance focused largely on areas specific to the new-tech sector, such as using modern marketing tools, including behavioural advertising (based on advanced profiling techniques) and remarketing conducted in cooperation with market-leading advertising networks, as well as combining/aggregating databases into groups of companies. He has also advised on the implementation of strategic projects, such as launching mobile applications or an advanced stationary biometric scanning technology, combined with an e-commerce account.
Jacek has conducted a number of audits in the field of personal data protection, and has helped raise the awareness of IT/TMT industry employees in order to practically implement data protection standards (through training for software developers and operations departments, including second-level).
He is associated with leading consulting companies in Poland and the Regional Chamber of Legal Advisers in Wrocław.

**Leśniewski Borkiewicz & Partners**
ul. Podwale 83 / 11
50-414 Wrocław
Poland

Tel: +48 793 967 934
Email: jc@lbplegal.com
URL: www.lbplegal.com/en

Leśniewski Borkiewicz & Partners (LB&P) is a modern law firm that works mainly with clients operating within IT, TMT and e-commerce. We know the specifics of the new technologies sector, and that allows us to propose practical solutions, taking into account typical risks, market practice and upcoming changes. LB&P has been created as a result of the further development of Leśniewski Legal. It has been formed by people with experience gained in one of the largest Polish advisory companies, as well as in specialised projects realised for international clients.
Our second brand privacyfoxes.com is dedicated to GDPR issues and implementing solutions for cross-border personal data flows.

**www.lbplegal.com/en**

Leśniewski Borkiewicz & Partners

# Russia

Klochenko & Partners Attorneys at Law

Lilia Klochenko

## 1 Relevant Legislation and Competent Authorities

### 1.1 What is the principal data protection legislation?

Federal Law No.152-FZ on Personal Data dated 27 July 2006 (the PD Law) is the key law governing data protection in Russia. It was adopted in 2005 following the ratification of the Convention of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data (the Strasbourg Convention).

The PD Law is based on the international instruments on privacy and data protection in certain aspects; it has concepts similar to the one contained in the General Data Protection Regulation (the GDPR) (effective in the EU since 25 May 2018).

### 1.2 Is there any other general legislation that impacts data protection?

Generally, the Russian Constitution recognises the fundamental right to privacy for each particular individual (Articles 23 and 24).

Specifically, the principal national privacy and data protection legislation is contained also in the Federal Law No.149-FZ on Information, Information Technologies and Data Protection (2006) (the Data Protection Act).

Finally, the Strasbourg Convention ratified by Russia in 2005 protects and enforces data protection at the international level.

The Russian data protection regulation places special emphasis on the technical measures for data protection. The numerous legal and technical requirements are set out in regulations issued by the Russian government and specialised governmental authorities in the data protection sphere.

### 1.3 Is there any sector-specific legislation that impacts data protection?

Specific data protection provisions can be found in other laws, including Chapter 14 of the Russian Labour Code (2001), Article 85.1 of the Russian Air Code (1997), Federal Law No.395-1 On Banks and Banking (1990), Federal Law No.323-FZ on the Fundamentals of Protection of the Health of Citizens in the Russian Federation (2011), Federal Law No.38-FZ on Advertising (2006), the Russian Administrative Offences Code (2001), etc.

### 1.4 What authority(ies) are responsible for data protection?

The principal local data protection regulatory authority is the Federal Service for Communications, Information Technology and Mass Communications Supervision (*Roskomnadzor*).

The specialised governmental authorities in the data protection sphere also include the Federal Service for Technical and Export Control (FSTEK) and the Federal Security Service (FSS).

## 2 Definitions

### 2.1 Please provide the key definitions used in the relevant legislation:

- "**Personal Data**"
  Personal data is defined as any information relating directly or indirectly to identified or identifiable individual (the personal data subject).
- "**Processing**"
  Processing is defined as any action (operation) or a set of actions (operations) towards personal data performed both automatically and manually, including the collection, recording, systematisation, accumulation, storage, specification (updating, modification), extraction, use, transfer (dissemination, provision, access), anonymising, blocking, deletion or destruction of personal data.
- "**Controller**"
  Russian law does not contain the concept of and term "controller". The Russian PD Law refers to the concept of "data operator", which may be a state agency, municipal authority, legal entity or individual who organises and/or carries out (alone or jointly with other persons) the processing of personal data and which also determines the purposes of personal data processing, content of personal data and actions (operations) related to personal data.
- "**Processor**"
  Russian law does not contain the concept of or term "processor"; however, it does refer to the concept of "data operator", to a party that may be acting (processing personal data), subject to data subject's consent, under the authorisation of the data operator on the basis of the corresponding agreement or by operation of the special state or municipal act.

- "**Data Subject**"
  A data subject is defined as a particular or identifiable individual (physical person).
- "**Sensitive Personal Data**"
  Instead of the term "sensitive personal data", the PD Law operates by the term "special categories of personal data", which refers to any information that relates to racial or ethnic origin, nationality, political opinions, religious or philosophical beliefs, state health or sexual life.
- "**Data Breach**"
  Russian legislation does not specify the term "data breach". However, processing of data in breach of principles and obligations stipulated in the PD Law could be qualified as a data breach.
- *Other key definitions – please specify (e.g., "Pseudonymous Data", "Direct Personal Data", "Indirect Personal Data")*
  - "Biometric personal data information" is a separate kind of information in relation to a person's physiological and biological characteristics from which he/she is identifiable and which is used by an operator to establish the identity of a personal data subject (Article 11 of the PD Law).
  - "Cross-border transfer of personal data" refers to any transfer of personal data to a foreign state, foreign state agency and/or foreign physical or legal person.

## 3 Territorial Scope

**3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?**

As stated in para. 1 of Article 12 of the PD Law, the cross-border transfer of personal data into the territories of foreign states which are parties to the Council of the Strasbourg Convention, as well as other foreign states providing adequate protection of data subjects' rights, shall be carried out in accordance with the PD Law and may be prohibited or restricted for the purposes of protecting the fundamentals of the constitutional order of the Russian Federation, public morality and health, rights and legitimate interests of citizens and providing for national defence and state security. *Roskomnadzor* approves the list of foreign states that are not parties to the Council of the Strasbourg Convention and that provide adequate protection of the data subjects' rights.

An operator shall receive its customers' permission to transfer their personal data to third parties and abroad.

Moreover, as per para. 5 of Article 18 of the PD Law, when collecting personal data, including via the internet, an operator (both Russian and foreign one) shall record, systemise, accumulate, store, specify (update, modify) or retrieve the personal data of Russian citizens by using any databases located in the Russian Federation, with the exception of data processing for state purposes or in the mass media. At the same time, an operator does not need to delete similar data from any foreign databases containing data on Russian citizens.

## 4 Key Principles

**4.1 What are the key principles that apply to the processing of personal data?**

- **Transparency**
  A personal data subject shall decide whether or not to provide his personal data for processing. He/she has the right to know the purposes and methods of processing of personal data, the name and location of the data operator, the recipients of personal data, the persons who have access to personal data, the term of processing and retention of personal data, and any other information required to ensure the transparent processing of personal data. Thus, the personal data subject shall give consent to the data operator. Such consent to the processing of personal data shall be specific, informed and conscious. The obligation to provide evidence of obtaining the personal data subject's consent shall be imposed on the operator.
- **Lawful basis for processing**
  Personal data shall be processed on a legal and fair basis. In particular, the processing of personal data shall be made with the data subject's consent (unless certain legal exemptions are applicable), which shall be granted freely, of the data subject's own will and in the data subject's own interest; the data operator or other person(s) who have obtained access to personal data shall not disclose or distribute such personal data to third parties without a data subject's consent, unless otherwise provided by the law.
- **Purpose limitation**
  Personal data processing should be limited to achieving objectives (purposes) which must be specific, predefined, and legitimate. Processing that is not consistent with the purposes of such processing is prohibited.
- **Data minimisation**
  The scope and content of personal data to be processed shall fully comply with the intended purposes of such data processing. The personal data to be processed shall not be excessive or irrelevant to the declared purposes of data processing.
- **Proportionality**
  Personal data processing should ensure that such personal data are accurate, sufficient, adequate and relevant and, where necessary, kept up to date in proportion to the purposes of data processing. The data operator must take all necessary measures or secure the performance of measures related to the deletion or correction of incomplete or inaccurate personal data.
- **Retention**
  Personal data which is processed shall be destructed or depersonalised upon achieving the purpose of data processing, as well as in case the achievement of such purposes is no longer effective, relevant or necessary, unless otherwise provided by the federal law.
- *Other key principles – please specify*
  Any integration of databases which contain personal data being processed for inconsistent purposes is not permitted.

## 5 Individual Rights

**5.1 What are the key rights that individuals have in relation to the processing of their personal data?**

- **Right of access to data/copies of data**
  In accordance with para. 1 of Article 14 of the PD Law, an individual has the right to access his/her data being processed by the data operator, including information containing: (1) confirmation the fact that his/her personal data are processed by the data operator; (2) the legal grounds for and purposes of the processing of the personal data; (3) the purposes and methods used by the data operator for the processing of personal data; (4) the name and location of the data operator and information on persons

who have access to personal data or to whom personal data may be disclosed based on the agreement with the data operator or on the law; (5) the processed personal data relating to the personal data subject in question and the source from which they were obtained; (6) the period of personal data processing, including the storage period; (7) the procedure for the exercise by the personal data subject of the rights provided for in the PD Law; (8) information on any actual or intended cross-border transfer of personal data; (9) the name (surname, first name and patronymic) and address of the person carrying out the processing of personal data on the instruction of the operator, if applicable; and (10) any other information provided for by the PD Law.

- **Right to rectification of errors**
  A personal data subject may request the data operator to rectify, block or delete his/her personal data in case they are incomplete, irrelevant, inaccurate or unlawfully obtained, or are not needed for the stated purpose of their processing.
- **Right to deletion/right to be forgotten**
  The Russian law sets forth the right to be forgotten by providing a pre-trial mechanism limiting dissemination of links to websites containing individual's information which is false, out of date or disseminated in violation of the laws (para.1 of Article 10.3 of the Data Protection Act). An individual has the right to demand, by sending the appropriate application, that an internet search engine operator discontinue providing links that permit access to information regarding that individual. At the same time, this mechanism does not limit an access to the resources themselves that actually disseminate information. If an individual is not satisfied with the outcome of the pre-trial settlement, he/she has the right to apply to the court with a statement of claim to limit issuing links to websites containing the individual's information.
- **Right to object to processing**
  Upon the request of a data subject, including instances wherein a personal data subject withdraws his/her consent to the personal data processing, a data operator shall be obliged, immediately to terminate the processing of his/her personal data. Except where the personal data processing cannot be terminated or would result in violation of the law (e.g. labour law), the data operator must discontinue the data processing or arrange for it to be terminated.
- **Right to restrict processing**
  In Russian legislation, there is no clear distinction between the right to restrict and the right to object, as provided for in the GDPR.
- **Right to data portability**
  A personal data subject has the right to access his/her personal data. The information should be provided in an accessible form. The law does not prohibit the transfer of personal data to other operators.
- **Right to withdraw consent**
  In the event that a personal data subject withdraws his/her consent to the processing of personal data, the data operator shall terminate the processing of the personal data or arrange for it to be terminated and, if the personal data no longer need to be kept for the set purposes of their processing, destroy the personal data or arrange for them to be destroyed within a period not exceeding 30 days from the date of receipt of the withdrawal, unless otherwise provided by a contract (paras 5 and 6 of Article 12 of the PD Law).
- **Right to object to marketing**
  The processing of personal data for marketing/promotion of goods, works and services directly to potential consumers (via telephone, email or fax) shall be permitted only under the preliminary consent of the personal data subject. The burden of proof that the data subject's consent has been duly received rests with the data operator. The Federal Law on Advertising also prohibits electronic publications and bulk mail without the prior consent of an addressee. The person shall have the right to withdraw consent at any time. If so requested by the personal data subject, the data operator must immediately discontinue the processing of her/his personal data.
- **Right to complain to the relevant data protection authority(ies)**
  If a personal data subject believes that a data operator is processing his/her personal data in violation of the data protection legislation or otherwise infringing upon his/her rights and freedoms, the personal data subject has the right to submit a complaint against the actions or inaction of the data operator to the *Roskomnadzor* or to bring a civil action with the competent court. The data subject may seek various legal remedies, including the reimbursement of losses, as available under the law.
- *Other key rights – please specify*
  The law prohibits any legally significant decisions from being taken in respect of a personal data subject solely on the basis of automated data processing. The exemption to this rule is when the subject of the personal data has given his written consent or in cases provided for by federal laws also establishing measures to ensure the observance of the rights and legitimate interests of the personal data subject. The data operator is obliged to explain to the personal data subject the procedure for making a decision on the basis of solely automated data processing and the possible legal consequences of such a decision.

## 6 Registration Formalities and Prior Approval

### 6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

The data operator should notify the *Roskomnadzor* before commencing processing of any personal data, and the data operator's details should be entered into a public register of personal data operators (https://rkn.gov.ru/personal-data/register/). The notification may be submitted electronically or on paper. The notification is not required in certain cases: where processing is carried out solely in accordance with the labour laws; if only subjects' full names are processed; where generally accessible or publicly available personal data are processed; or where personal data processing is carried out for the purposes of providing a personal data subject with a single-entry pass to protected premises.

### 6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

The notification of the *Roskomnadzor* must be specific and shall be signed by an authorised person of the applicant.

**6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?**

The notification shall be made per processing purpose.

**6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?**

Local legal entities, foreign legal entities or their representative offices, subject to the relevant data protection legislation, must notify the data protection authority.

**6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?**

The notification of the *Roskomnadzor* must specify: the name and address of the data operator; the name and contact details of the data protection officer; the purpose of the personal data processing; the categories of data to be processed; the categories of the prospective data subjects, whose data is being processed; the data source; the processing activity; the legal basis of the processing of personal data; the list of actions to be performed in relation to personal data processing and the description of methods of processing of personal data; the description of IT systems and security measures; the start date of data processing; the term of processing or the condition for termination of processing personal data; the location of the personal databases; and the cross-border data transfer intention.

**6.6 What are the sanctions for failure to register/notify where required?**

The Russian Code of Administrative Offences imposes liability for failure to file or late filing to *Roskomnadzor* of notification on data processing activities (Article 19.7) with a fine of RUB 3,000 to 5,000 for the legal entities and RUB 300 to 500 for their officials.

**6.7 What is the fee per registration/notification (if applicable)?**

There is no registration or notification fee.

**6.8 How frequently must registrations/notifications be renewed (if applicable)?**

There is no obligation to regularly renew information; however, the data operator must notify *Roskomnadzor* of any amendments of information provided to the register within 10 working days from the date such amendments arise.

**6.9 Is any prior approval required from the data protection regulator?**

No prior approval is required from the data protection regulator in order to perform data processing activity.

**6.10 Can the registration/notification be completed online?**

The notification can be completed online at the official website of the *Roskomnadzor*.

**6.11 Is there a publicly available list of completed registrations/notifications?**

The register of operators is publicly available on the official website of the *Roskomnadzor*.

**6.12 How long does a typical registration/notification process take?**

The *Roskomnadzor* shall, within 30 days from the date a notification is filed, enter the details of the applicant in the register of operators.

## 7 Appointment of a Data Protection Officer

**7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.**

According to the Russian legislation, the data operator, which is a legal entity, shall appoint a person responsible for organising the personal data processing (Article 22.1 of the PD Law), who, within the meaning of the function performed, is a Data Protection Officer.

**7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?**

There are no specific sanctions for failing to appoint a Data Protection Officer. At the same time, the *Roskomnadzor* is entitled to carry out inspections over the application of the PD Law by operators. In case of violation of laws, the *Roskomnadzor* is entitled to issue binding orders to remedy the violation and may also apply the corresponding fines.

**7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?**

The Data Protection Officer is not excluded or protected from disciplinary measures or other employment consequences in respect of his/her functions as a Data Protection Officer.

**7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?**

Yes; a single Data Protection Officer might be appointed to cover multiple entities.

**7.5 Please describe any specific qualifications for the Data Protection Officer required by law.**

The Russian law does not set any specific qualifications for the Data Protection Officer. However, the Data Protection Officer must have good general knowledge of data protection legislation.

**7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?**

The Data Protection Officer shall be obliged, in particular, to exercise internal control over the compliance by the data operator and its employees of the data protection legislation, to inform the employees of the data operator about the relevant provisions of the data protection legislation, by-laws, local rules or acts on personal data processing, and any requirement on data protection, and to organise the acceptance and processing of requests of the data subjects or their representatives and to perform necessary control over their processing. Other functions and responsibilities may be provided by the internal corporate or governance rules or acts of a data operator.

**7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?**

The Data Protection Officer shall be named in the notice to the *Roskomnadzor* and recorded in the register of data operators.

**7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?**

No, this is not necessary, excluding the requirement to be specified in the notice to the *Roskomnadzor*.

## 8 Appointment of Processors

**8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?**

A data operator has the right to assign the processing of personal data to another person who might carry out the processing of personal data on behalf and under the instructions of a data operator (third parties acting on an instruction of a data operator). A data operator and a third party acting on an instruction of a data operator for carrying out the processing of personal data shall enter into an agreement thereon.

**8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?**

An agreement shall be in writing and signed by the parties' authorised persons. Such agreement shall set out a list of actions to be performed when processing the personal data by the person carrying out processing, and the purposes of processing. It shall also establish the obligation of the person performing data processing to observe the principles of security and confidentiality of personal data, as well as the liability for non-compliance with them.

## 9 Marketing

**9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).**

The processing of personal data for the purpose of the marketing/promotion of goods, works and services, directly with a potential consumer (whether sent by telephone, email, or SMS), without prior consent of the subject of the personal data or addressee of advertising, is unauthorised and therefore not permitted. The burden of proof that the prior consent of the personal data subject or addressee was duly issued rests with the data operator. The data subject's or addressee's consent may also be revoked, in which case the data operator or advertising distributor shall immediately terminate any marketing communications to avoid the breach.

**9.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?**

The restrictions of the PD Law apply only to business-to-consumer marketing. The restrictions of the Federal Law on Advertising (bulk mail) can apply also to business-to-business marketing/promotion.

**9.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).**

Any distribution of advertisements via electronic communication networks, including telephone, fax and mobile telephone communication, is only admissible if the addressee has granted his/her consent to receive such advertisements. The distributor of an advertisement shall immediately terminate distributing the advertisements to a person who requested to do so. It is prohibited to market by using automatic dial-up or automatic mailing facilities (Article 18 of the Federal Law on Advertising).

**9.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?**

The above-mentioned rule is general and applies with no exceptions for foreign entities.

**9.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?**

The Federal Antimonopoly Service is an authorised federal executive body, which exercises functions in relation to advertising. In accordance with the Consumer Protection Act (1992), the Federal Service for the Protection of Consumer Rights and Human Wellbeing (also known as "*Rospotrebnadzor*") shall also protect consumers against intentionally imposed services sent by electronic means.

**9.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?**

In general, individuals must give prior written consent for entering his/her name and other details into the purchase marketing list or request them to be deleted thereof. The burden of proof that the prior consent of the addressee of advertising was duly issued rests with an entity or person who purchased marketing lists containing personal data from third parties.

**9.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?**

The fine for the electronic marketing/promotion of goods, works or services in breach of the relevant consumer protection legislation, in particular, without a prior consent of addressee, may lead to an administrative fine up to RUB 500,000 for legal entities and up to RUB 20,000 for their officials (Article 14.3 of Russian Code of Administrative Offences).

## 10 Cookies

**10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).**

Russian law does not contain a definition of cookies or any specific regulation with regard to cookies. There are no official guidelines from *Roskomnadzor* or other state agency on using or distributing of cookies, except brief reference in the Professional Standards of the Labour Ministry for IT specialists regarding the scope of knowledge and the use of cookies. If cookies or similar technologies are used by the data operator for authenticating the user, storing his/her account, personal preferences and settings, or tracking the status of a customer's access session for marketing purposes, all of these uses can be qualified as the processing of personal data for the purpose of the marketing/promotion of goods, works or services, which requires a customer's prior consent (Article 15 of the PD Law).

**10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?**

There are no restrictions which distinguish between different types of cookies; the relevant factor is the possibility of identifying a user.

**10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?**

Currently, the practice is developing where *Roskomnadzor* brings enforcement actions in the Russian courts, including in relation to cookies.

**10.4 What are the maximum penalties for breaches of applicable cookie restrictions?**

Since cookies are considered marketing communications, any breach of relevant data protection and advertising or telecommunication regulation shall entail administrative penalties as applicable for personal data infringements.

## 11 Restrictions on International Data Transfers

**11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.**

The PD Law provides for the local storage requirement, which applies to any data operator that processes the personal data of Russian citizens, regardless of its jurisdiction, and including its online business activity. Thus, when collecting personal data, including via the internet, an operator must record, arrange, accumulate, store, specify (update, change) or retrieve the personal data of citizens of the Russian Federation by using any databases physically located in the Russian Federation, with the exception of: the processing of data in order to achieve the objectives of international treaties or the implementation of an operator's statutory powers and duties; for state purposes; for professional activities of journalists or the lawful activities of mass media; or scientific, literary or other creative activities that may be performed directly in the foreign databases (Article 18(5) of the PD Law).

In the event of a cross-border transfer of personal data, a data operator, before such transfer, must ensure that the rights and interests of the respective data subject are fully protected in the "adequate manner" in the corresponding foreign country (Article 12 of the PD Law). All countries that are signatories to the Strasbourg Convention are regarded as the jurisdictions providing "adequate protection" of rights and interests of data subjects. In addition, *Roskomnadzor* has adopted an official list of countries which are not signatories to the Strasbourg Convention but secure "adequate protection" for the purposes of cross-border transfers of personal data. International data transfer to any jurisdiction with the "adequate protection" level is not subject to any restriction, provided that the prior consent of the respective data subject has been received by the data operator. In addition, the PD Law set forth special requirements for the cross-border transfer of personal data to countries which do not provide the level of "adequate protection".

**11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).**

In practice, prior to transferring personal data abroad, the data operator should first check the level of data protection in a respective foreign jurisdiction. Further, prior written consent from the respective data subjects is required in order to transfer personal data to other jurisdictions. The data operator may also execute an international data transfer agreement with the personal data subject.

**11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.**

The cross-border transfer of personal data does not require any registration or prior approval by *Roskomnadzor*. However, the notification to *Roskomnadzor* for the purposes of registration of the status of a data operator shall contain information on whether a cross-border transfer of personal data will occur during its processing.

**11.4 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?**

There is no such guidance issued by the Russian data protection authority.

**11.5 What guidance (if any) has/have the data protection authority(ies) issued in relation to the European Commission's revised Standard Contractual Clauses?**

There is no such guidance issued by the Russian data protection authority.

## 12 Whistle-blower Hotlines

**12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?**

Russian legislation does not include any specific regulation on corporate whistle-blower hotlines. Furthermore, there is no binding guidance issued by *Roskomnadzor* in this regard. General requirements of personal data legislation shall apply. Employees may be also obliged to "blow the whistle" under the internal corporate rules or policies of the employer as a data operator.

**12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?**

Anonymous reporting is not prohibited or strongly discouraged under the applicable laws. Commonly, the data operators address this issue in their internal corporate rules or policies.

## 13 CCTV

**13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?**

CCTV does not require separate notification/registration or prior approval from *Roskomnadzor*. In certain circumstances, the trafficking or use of special technical equipment intended for secretly obtaining information may become a ground for imposing a criminal liability (Article 138.1 of the Russian Criminal Code). However, such special technical equipment does not include items with audio, video, or photo recording and/or geolocation functions for domestic purposes which have controls, indications and/or any marks openly indicating their purpose, function and/or mode of work.

**13.2 Are there limits on the purposes for which CCTV data may be used?**

The Russian Constitution guarantees the right to privacy and to personal and family confidentiality. Thus, it should be assessed whether this right has been violated on a case-by-case basis.

## 14 Employee Monitoring

**14.1 What types of employee monitoring are permitted (if any), and in what circumstances?**

In practice, different types of employee monitoring may be permitted under the internal corporate rules and policies of employers, including video surveillance, email/internet browsing, social media monitoring and audio listening, as well as GPS tracking, occasionally. However, in any such monitoring, the employer (data operator) must observe the constitutional rights of citizens and data protection requirements (para. 1 of Article 24 of the Russian Constitution). The employer may apply any type of employee monitoring provided that this is stipulated by an employment agreement or regulated under the internal corporate rules or policies, the employees are familiar with them in advance of application, and employees have given their consent to such surveillance. Any employee monitoring should be applied reasonably and any disclosure of video content to third parties should be avoided.

**14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.**

The prior written consent of an employee is required to perform legal employee monitoring. In practice, the written consent from all employees is obtained at the time of the execution of employment agreements or is a part of collective employment arrangement. All employees should be duly acquainted with the internal corporate rules and policies in relation to employee monitoring measures. The legislative provisions regarding the processing of employees' personal data shall also be observed. In particular, such personal data processing can be carried out exclusively for the purpose of ensuring compliance with laws and other regulatory legal acts, ensuring the personal safety of employees, assisting employees in employment, monitoring the quantity and quality of work performed and ensuring the safety of property, etc. (Article 86 of the Russian Labour Code). For those specific purposes, additional consent is not required. The written consent of an employee is required and shall be obtained in advance by the employer if personal data need to be transferred by the employer to third parties.

**14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?**

There are no special requirements that works councils/trade unions/employee representatives need to be notified or consulted in this regard.

## 15 Data Security and Data Breach

**15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?**

A data operator or other person(s) who have obtained access to personal data shall be obliged to refrain from disclosing them to third parties or disseminating those personal data without the prior written consent of the personal data subject, except where provided by federal laws.

**15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

Generally, there are no legal requirements to report data

breaches to the data protection authority. The *Roskomnadzor* shall examine claims voluntarily brought by a personal data subject in respect of compatibility of the content of personal data, existing or lack of the personal data subject's consent, methods of personal data processing and its compliance with the declared purposes for which they are processed. The *Roskomnadzor* shall adopt an appropriate decision on that and, if the violation is detected, the data operator must terminate such unauthorised processing within three business days. In case it is not possible to turn the unauthorised processing of personal data into a legitimate processing manner, the data operator must destroy such personal data within 10 business days (Article 21(3) of the PD Law). The data operator must notify the data subject or its representative on termination of the processing or destruction of personal data and, in the event the request for termination or destruction has been made by the *Roskomnadzor*, such notification must be sent to the *Roskomnadzor*.

**15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

There is no special legal requirement to report data breaches to affected data subjects. At the same time, a personal data subject whose rights have been infringed is entitled to submit a claim to the *Roskomnadzor* who might exercise a relevant inspection and adopt its decision in respect of the alleged infringer and its unauthorised actions with personal data.

**15.4 What are the maximum penalties for data security breaches?**

A data operator may be liable for several breaches of personal data processing – including for data processing without the data subject's written consent when required, failure to publish the policy on data processing on the website, or failure to provide the data subject with the information related to the processing of his/her personal data – with fines for an offence up to RUB 75,000 (Article 13.11(2) of the Russian Code for Administrative Offences).

The data operator may be subject to fines of up to RUB 6,000,000 for the first-time offence, and up to RUB 18,000,000 for the second-time offence of non-compliance with the local storage requirement (Article 13.11(8&9) of the Russian Code for Administrative Offences).

Finally, the Russian Criminal Code provides criminal liability for: unlawful collection or dissemination, including public dissemination, of personal data related to a personal or family secret without that individual's consent, with a fine up to RUB 200,000; and illegitimate access to computer information that has caused the destruction, blocking, modification or copying of personal data, with a fine up to RUB 500,000. It should be noted that under Russian law, criminal penalties can be imposed only on individuals and not on legal entities.

## 16 Enforcement and Sanctions

**16.1 Describe the enforcement powers of the data protection authority(ies).**

(a) **Investigative Powers**: The *Roskomnadzor* has the following investigative powers: to request and obtain necessary information in order to exercise its powers, and to receive such information free of charge; to check information contained in a notification on the processing of personal data and enter such information into the register of data operators; to exercise the relevant inspections; and to send materials to public prosecution bodies and other law enforcement authorities.

(b) **Corrective Powers**: The *Roskomnadzor* has the following corrective powers: claiming rectification, blocking or destruction of false or illegally obtained personal data; limiting access to data that is processed under the breach of data protection legislation; and suspending or terminating the processing of personal data that has been initiated under the breach of the data protection legislation.

(c) **Authorisation and Advisory Powers**: The *Roskomnadzor* has no special authorisation powers except for the entering of the data operator into the register of personal data operators, which is a legal basis for exercising the right to the processing of personal data, although it may send an application to the body licensing the operator's activities (such as the Federal Service for Technical and Export Control, the Federal Security Service and other state agencies) to consider the issue of taking measures to suspend or cancel the relevant license as prescribed by the applicable law if one of the conditions of the license to carry out such activities is a ban on the transfer of personal data to third parties without written consent from the subject of personal data. When performing its advisory powers, the *Roskomnadzor* may issue the explanatory letters or by-laws or acts within its competence, as well as submit to the Government of the Russian Federation proposals on improving the legal regulation of the protection of the rights of data subjects.

(d) **Imposition of administrative fines for infringements of specified GDPR provisions**: The *Roskomnadzor* has the power to take administrative action against persons guilty of violating the PD Law, in particular by imposing administrative fines for infringements of the personal data subject's right or violation of other relevant legislative provisions.

(e) **Non-compliance with a data protection authority**: In case of non-compliance with the *Roskomnadzor*'s decisions or binding orders, the *Roskomnadzor* may bring civil actions with competent courts for the protection of rights of data subjects and representing the interests of data subjects before the trial or send materials to the Prosecutor's Office and other law enforcement agencies for the purposes of commencement of criminal cases for the data breaches.

**16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?**

The *Roskomnadzor* is entitled to require a data operator to stop a particular infringement or violation, including a particular processing activity, such as blocking its website or particular pages on the internet. A court decision for such measures is required.

**16.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.**

In case of any violation, the *Roskomnadzor* first sends a warning with the relevant prescriptions on measures to be taken in order to stop such violation. The case law in Russia in this regard is still forming. In 2020, for example, a Russian court fined

Twitter and Facebook the amount of RUB 4,000,000 each for their refusals to locate their servers' holding data about Russian citizens on Russian territory. There are also numerous completed or outstanding cases related to Telegram Messenger; in particular, the use of Telegram-bots to collect the personal data of Russian citizens.

**16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?**

The *Roskomnadzor* may block access to information processed in violation of the personal data laws; for example, following the failure to fulfil the personal data localisation requirement, LinkedIn was blocked in 2016.

## 17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

**17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?**

Russian law does not contain any provisions related to foreign e-discovery or foreign disclosure proceedings. Therefore, Russian companies are not obliged to respond to foreign e-discovery or disclosure requests unless there are imperative provisions set forth by the corresponding international treaties on mutual legal support (assistance) or similar international agreements to which Russia is a party. In addition, there is a practice whereby companies respond to foreign requests for disclosure from foreign law enforcement agencies through the competent Russian authorities.

**17.2 What guidance has/have the data protection authority(ies) issued?**

No such guidance has been issued by the *Roskomnadzor*.

## 18 Trends and Developments

**18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.**

Privacy and data protection remains an emerging and trending area of legislation development in Russia. There is a noticeable tendency to increase fines for data protection infringements to make them more consistent with foreign legislation.

**18.2 What "hot topics" are currently a focus for the data protection regulator?**

From the very recent legislation development, foreign internet sites, web pages, information systems and programmes aimed at Russian users may be required to open local offices in accordance with a draft law being considered by the Russian Parliament. In the coming future, the *Roskomnadzor* may impose the new requirements on individual hosting providers, information distribution organisers or advertising system operators. There are also various initiatives on the introduction and implementation of the concept of "Big Data" and establishing the rights of users when their personal data are used in such a way.

**Lilia Klochenko** holds a Law degree and Ph.D. *jur. cum laude* from MGIMO, is certified for international arbitration from the ICC Advanced Arbitration Academy, and is a Russian qualified attorney-at-law.
Lilia has specific industry expertise, in particular in data protection, confidential information and privacy compliance, e-commerce, corporate governance and compliance, financial and tax issues, as well as competition law issues.
Lilia consults in the areas of intellectual property, information technologies and communications, as well as data protection legal control and compliance. She also has experience in the development of data protection guidance and policies, including privacy policies and exercising due diligence of intellectual property items.
Lilia is a certified international arbitrator and strongly focuses her practice on litigation and alternative dispute resolution, both international and domestic arbitrations, acting in a capacity of an arbitrator or counsel (representative), including for data protection disputes.

**Klochenko & Partners Attorneys at Law**
Office 523, 13
Building 43, 2nd Zvenigorodskaya Street
Moscow 123022
Russia

Tel: +7 903 775 6020
Email: klochenko@2klegal.com
URL: www.2klegal.com

Klochenko & Partners Attorneys-at-Law was established by lawyers who unite Russian wisdom, European divergence and English pragmatism, having over 20-years' experience in legal practice within broad competencies, including extensive and varied experience in providing legal support on personal data and confidential information and protecting intellectual property. Being a full-service boutique law firm with a primary focus on providing practical and financially beneficial legal services by taking an objective and proactive approach, the firm advises its client across a wide range of compliance issues. Among the firm's clients are major brand owners, software developers, advertising companies, licensing agencies and online shops. While dealing with a complex legal issue, the firm keep clients aware of all the nuances and complexities of each situation to build trusted and efficient relationships.

**www.2klegal.com**

# Saudi Arabia

Hammad and Al-Mehdar Law Firm

Suhaib Hammad

## 1 Relevant Legislation and Competent Authorities

### 1.1 What is the principal data protection legislation?

At the time of writing, there is no specific law regulating data protection in the Kingdom of Saudi Arabia (the "*Kingdom*"). However, the Saudi Authority for Data and Artificial Intelligence ("*SADAIA*") is in the process of preparing the draft regulations and it is reasonably anticipated that the initial draft will embody similar protections as those adopted by the Abu Dhabi Global Market authority and the EU General Data Protection Regulation ("*GDPR*"). It is important to note that Shariah and Islamic principles protect the individual's right to privacy and prohibit any action that may invade such privacy. These principles prohibit disclosure of personal information without the consent of the individual unless public interest requires such disclosure. There are other sector-specific regulations that are meant to protect the individual's data, such as the Electronic Commerce Law and the Electronic Transactions Law and its Implementing Regulations. Additionally, the Communication and Information Technology Commission ("*CITC*") issued rules such as the General Principles, which aim to protect the data of users of electronic services and regulate the obligations of the service providers.

### 1.2 Is there any other general legislation that impacts data protection?

- The Electronic Commerce Law and its Implementing Regulations issued by Royal Decree No. (M / 126) dated 7/11/1440 AH (the "*E-Commerce Law*");
- the Electronic Transactions Law and its Implementing Regulations issued by Royal Decree No. (M / 18) dated 8/3/1428 AH (the "*E-Transactions Law*");
- the Payment Service Provider Regulatory Guidelines issued by the Saudi Central Bank (known as "*SAMA*") in January 2020 (the "*PSP Guidelines*");
- the General Principles for Personal Data Protection issued in April 2020 AD by the CITC;
- a guide to assessing privacy risks for telecom and IT providers and post issued by the CITC in December 2020 (the "*Privacy Risk Assessment Guide*");
- the CITC also issued the Procedure of Launching Services or Products Based on Customers, Personal Data, or Sharing Personal Data in May 2020 AD; and
- the Anti-Cyber Crime Law issued by Royal Decree No. (M / 17) dated 8/3/1428 AH.

### 1.3 Is there any sector-specific legislation that impacts data protection?

- The E-Commerce Law, which aims to: (i) control all electronic transactions between consumer and merchant; (ii) protect consumer data; and (iii) clarify the merchant's obligation and regulatory procedures to carry out the e-commerce activities in the Kingdom. Article 5 of the E-Commerce Law imposes the merchant to take all necessary measures to protect consumer data and dispose it upon completion of transaction, unless agreed otherwise.
- The E-Transactions Law aims to establish unified legal rules for all use of electronic transactions in public and private sectors. It was issued with the purpose of protecting data by imposing certain obligations to internet service providers such as privacy of information collected in the course of their business, regardless of its reference to public or private sector.
- Anti-Cyber Crime Law aims to reduce the occurrence of cyber crimes through defining what constitutes a crime and the relevant penalties applicable for this crime. The law aims to protect public security through achieving information security and preserving the rights arising from any electronic transaction or uses.
- The General Principles lay down the foundations, principles and also obligations towards data protection for telecom and IT service providers in the Kingdom and aim to protect personal data collected and processed during electronic transactions and services.
- The Procedures of Launching Services or Products Based on Customers, Personal Data or Sharing Personal Data have been issued to organise services depending on the use of personal data. The Procedures explain the mechanism to be followed for the purpose of sharing personal data with third parties.

### 1.4 What authority(ies) are responsible for data protection?

In an effort to regulate data collection and usage, SADAIA was established in August 2019 pursuant to Royal Order No. (74167) and is chaired by the Board of Directors' Deputy Prime Minister of Saudi Arabia in line with the objectives of the Kingdom's vision 2030. SADAIA is an independent authority responsible for regulating and overseeing data collection and processing in the Kingdom. There are three other bodies connected to it: the National Centre for Artificial Intelligence; the National Data Management Office; and an existing centre at the Ministry of

Interior, the National Information Centre. It is expected that SADAIA will play an independent role in overseeing matters related to personal data breaches and act impartially when performing its duties.

Furthermore, the CITC oversees compliance with data protection by service providers that are licensed by it.

Until the relevant data privacy regulation is issued, Article 23 of the E-Commerce Law states that dedicated employees shall be appointed for the purpose of monitoring data protection by virtue of ministerial decision. In case of any disputes arising, Article 22 of the same law states that the competent court shall rule over such disputes. At the time of writing, the supervising authority will differ depending on the nature of the claim and the jurisdiction it falls under.

## 2 Definitions

**2.1 Please provide the key definitions used in the relevant legislation:**

- "**Personal Data**"
  In reference to personal data, there is a definition given in the General Principles that apply to CITC licensed service providers in the Kingdom, which states the following: personal data refers to any information, regardless of its source of form, that would lead to identifying the customer, or that would render the customer identifiable directly or indirectly, including, but not limited to, names, ID numbers, address, contact numbers, licences and registration numbers and personal properties, bank account numbers and credit card numbers, customers' photos or videos, as well as any other data of personal nature.
- "**Processing**"
  Processing of personal data is also defined in the General Principles issued by the CITC as all processes performed on personal data, by any means, including but not limited to data collection, data transfer, storage and sharing, destruction, analysis, pattern extraction or drawing conclusions based on integrating them with other data.
- "**Controller**"
  There is no explicit definition at the time of writing. In reference to the CITC General Principles and Guidelines, a controller is the telecom and IT service provider offering the services.
- "**Processor**"
  Similarly, the CITC General Principles consider a processor any third party that processes the personal information on behalf of the controller (being licensed by the CITC).
- "**Data Subject**"
  The General Principles make reference to the "customer" whose data is collected and further processed, and this could be a natural or juridical person who uses any of the telecom, IT or postal services offered by the licensed service provider to whom the Principles apply.
- "**Sensitive Personal Data**"
  The current regulations in the Kingdom referred to in question 1.2 do not define "sensitive personal data". However, the Privacy Risk Assessment Guide refers to classes of sensitive data, which include age, children, and individuals with disabilities.
- "**Data Breach**"
  A data breach is, as defined in the General Principles that apply to CITC licensed service providers, any personal data disclosure, revealing, publishing, acquisition and authorising access without a legal basis intentionally or accidentally.
- *Other key definitions – please specify (e.g., "Pseudonymous Data", "Direct Personal Data", "Indirect Personal Data")*
  There are no other key definitions introduced under the existing regulations.

## 3 Territorial Scope

**3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?**

The CITC General Principles apply to licensed service providers that offer their services in another jurisdiction. Prior to offering any services in another jurisdiction, such service provider is required to obtain CITC consent and will remain subject to these principles.

There is no text that requires entities to carry out similar data protection measures as applied in the Kingdom when operating in other jurisdiction. We hope to see minimum protection requirements of cross-territorial data processing once the data protection regulation is issued.

## 4 Key Principles

**4.1 What are the key principles that apply to the processing of personal data?**

- **Transparency**
  Some key principles that apply to the processing of personal data are outlined in Article 4 of the General Principles. This requires service providers to follow specific guidelines when processing customers' personal data. Pursuant to Article 4 (1) of the General Principles, consumer data should be processed by service providers in a lawful and transparent manner in order to avert unjustified negative impact on customers' interests. Furthermore, the second paragraph of the same Article obliges the service provider not only to clearly specify the purposes for which the collected data shall be used, but to also inform the costumer whose data is being processed, emphasising the element of transparency.
  In addition to the above, Article 6 of the General Principles provides that users are granted the right to review and obtain a copy of their personal data before being processed and during the processing procedure at any time. This right is in line with Article 4 mentioned above with respect to ensuring that users are informed of their data that is being processed in an easy and accessible manner.
- **Lawful basis for processing**
  As previously stated, personal data shall be processed in a lawful manner, pursuant to Article 4 (1) of the General Principles.
- **Purpose limitation**
  According to Article 4 (2) of the General Principles, processing of customers' personal data shall be for specified and clear purposes that shall be further communicated to the customers. As such, not only do the principles provide limitation, but they also ensure transparency through obliging data processors to communicate the purpose of maintaining data to said users.
- **Data minimisation**
  When collecting customers' personal data, service providers shall be limited to what is necessary in relation to the purposes for which the data is being collected,

pursuant to Article 4 (3) of the General Principles. As such, data processors are expected to gather as little data as possible for the purpose of the desired transaction only.

- **Proportionality**
  The Kingdom's regulations do not address collection of personal data in proportion. However, it is implied that all data collected and processed is subject to the applicable regulations.
- **Retention**
  Regarding the retention of the personal data, Article 5 (5) of the General Principles obligates service providers to keep users' personal data for a specific purpose and period and, once said purpose and period are completed, the service provider shall ensure the deletion of all personal data. Additionally, according to Article 5 (1) of the E-Commerce Law, it is not permissible to retain consumer data except for the period that is dictated by the nature of electronic transactions. Thus, the laws in the Kingdom provide for a specific period to maintain personal data.
  Furthermore, Article 4 (4) of the General Principles states: "*[C]ustomers' personal data shall not be kept in a form that allows the identification of the customer for longer than is necessary to achieve purposes of personal data processing.*" As mentioned above, Article 4 of the General Principles lists several conditions that shall be complied with in order to maintain and preserve data, such as accuracy, clarity, and documentation standards to ensure the integrity of the data when preserving them.
- **Other key principles – please specify**
  Another key principle that applies for processing data in the Kingdom is the processing of data in a secure manner. The General Principles and E-Commerce Law both require security when processing data. Customers' personal data shall be securely maintained to ensure their protection and prevent unauthorised access thereto or breach, tampering, or misuse thereof, as per Article 4 (5) of the General Principles.
  Additionally, Article 4 of the General Principles lists several conditions that shall be complied with in order to maintain and preserve data, including that accurate, clear, and documented standards must be followed to ensure the integrity of the data when preserving them. Paragraph 3 of Article 5 (1) of the Implementing Regulations of the E-Transactions Law further obligates data processors to ensure the existence of effective plans for data recovery in the event of disasters. Hence, the law in the Kingdom obligates that data overserved are accurate, safely kept, and protected from any potential infringements and/or disasters.

## 5 Individual Rights

### 5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**
  Pursuant to Article 6 (4) of the General Principles, users in relation to the processing of their personal data must be able to obtain a copy of such data in an electronic format, in accordance with the CITC's instructions.
- **Right to rectification of errors**
  In relation to the right of rectification of errors, Article 6 (3) of the General Principles states that users must be granted the right to access their personal data that is being processed by the service provider at any time and correct such data when its incorrect or inaccurate.
- **Right to deletion/right to be forgotten**
  As mentioned above, users have the right to access their data at any time. Further, users have the right to withdraw their consent from sharing their data, which will oblige service providers to delete or erase said data, according to paragraph 1 of the same Article. Thus, users have the authority to either erase data during their correction process or withdraw their consent to share data, which will subject their data to erasure.
- **Right to object to processing**
  The right to object to data processing is not clearly tackled under the current regulations. We anticipate seeing this introduced once the data protection law is released.
- **Right to restrict processing**
  Data subjects and consumers do not have the discretion to restrict the processing of their data. The regulations only allow data subjects (consumers) the right to delete their data at any time they so desire. We hope to see more rights for data subjects under the data protection regulations once issued.
- **Right to data portability**
  The right to data portability is not clearly tackled under the current regulations. We anticipate seeing this introduced once the data protection law is released.
- **Right to withdraw consent**
  Article 6 (1) of the General Principles prohibits the processing of personal data prior to obtaining the users' explicit consent. Users are also able to withdraw their consent at any time should they wish to stop the processing of their data. As such, the law does empower users with the right to obtain confirmation in relation to any processing activity in addition to the right to withdraw their confirmation at any time.
- **Right to object to marketing**
  The preservation of consumer data shall be specifically for the purpose of fulfilling the obligation for which the data have been processed. Moreover, as per paragraph B of Article 5 (2) of the E-Commerce Law and its Implementing Regulations, service providers are restricted from using processed data for the purpose of advertising and marketing without obtaining the explicit consent of the concerned individual.
- **Right to complain to the relevant data protection authority(ies)**
  Data subjects have the right to complain about any breach to their data collected or processed by telecom and IT service providers. These complaints may be filed directly with the CITC.
  Similarly, data subjects and customers reserve the right to file a complaint to SAMA for any breach of their confidential or personal information by banks and financial institutions. These complaints may be filed online through https://www.samacares.sa and are directly managed by SAMA.
- *Other key rights – please specify*
  The E-Commerce Law provides limitation over the processing of an individual's personal data and the service provider shall be responsible for non-compliance in case of any breach to the data subject. According to Article 5 (2) of the E-Commerce Law, it is not permissible for service providers to process users' data for unauthorised purposes, and where data are to be used for purposes other than those previously communicated to the relevant users, such disclosure is subject to the consent of the concerned user.
  Further, the General Principles obligate CITC licensed service providers to implement a privacy programme to maintain customers' personal data protection pursuant to Section 5-1 of the Principles.

## 6 Registration Formalities and Prior Approval

**6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?**

CITC licensed service providers are required to immediately notify the CITC of any breach that has occurred in connection with customers' personal data subject to Section 5-6 of the General Principles. Similarly, SAMA, under the banking control department, oversees any violation, fraudulent activities, and breach of personal information by any bank or financial institution.

**6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?**

This is not clearly addressed under the current regulations. However, licensed service providers are required to notify the CITC of any data breach to customers' personal information. This notification must follow the approved mechanism and procedures by the CITC.

**6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?**

This is not clearly defined under the current regulations.

**6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?**

Considering that the current regulations apply differently to various sectors, some of these regulations specify the notification or registration requirement prior to any personal data processing. Therefore, licensed service providers in the telecom and IT sectors are required to directly notify the CITC.

Moreover, a licensed payment service provider must notify SAMA of any breach under the PSP Guidelines including a breach of the data privacy of its customers pursuant to Article 6.18 of the Guidelines.

**6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?**

There are no relevant details of the registration or notification requirements under the current regulations.

**6.6 What are the sanctions for failure to register/notify where required?**

There is no such clause under the current regulations. However, the regulations set out penalties for breaches made under its rules. Regarding the amount to be paid, even though it is defined under the regulations, the relevant authority may have the discretion to fine the service provider for breaches made under the said regulation within the permitted limits.

**6.7 What is the fee per registration/notification (if applicable)?**

This is not applicable.

**6.8 How frequently must registrations/notifications be renewed (if applicable)?**

This is not applicable.

**6.9 Is any prior approval required from the data protection regulator?**

This is not applicable.

**6.10 Can the registration/notification be completed online?**

The notification forms for any data breach by CITC licensed service providers or SAMA service providers (such as banks and financial institutions) are not made available online. However, we anticipate that these forms are shared with the service providers and submitted online.

**6.11 Is there a publicly available list of completed registrations/notifications?**

This information is not disclosed.

**6.12 How long does a typical registration/notification process take?**

This information is not disclosed.

## 7 Appointment of a Data Protection Officer

**7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.**

Until the draft data protection regulations are put in place, Article 23 of the E-Commerce Law governed by the Ministry of Commerce provides that dedicated employees for the purpose of monitoring data protection and privacy shall be appointed by virtue of a ministerial decision.

**7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?**

The current regulations do not require the appointment of a Data Protection Officer.

**7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?**

This is not applicable.

**7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?**

This is not applicable.

**7.5 Please describe any specific qualifications for the Data Protection Officer required by law.**

This is not applicable.

**7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?**

We expect that the data protection regulation, once issued, will adopt international practice similar to the GDPR and other regulations.

**7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?**

This is not applicable.

**7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?**

At the time of writing, there is no such requirement.

## 8 Appointment of Processors

**8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?**

At the time of writing, the General Principles that apply to CITC licensed service providers state in Article 6 (1) that the data subject whose data is being processed must give his explicit consent. Further, any processing of a data subject's personal information through a processor must be notified to the CITC. This must be done by completing Annex 2 (CITC notification form) of the Privacy Risk Assessment Guide.

**8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?**

CITC licensed service providers are required to adhere to the utmost protection level of data privacy. This is particularly implemented due to the nature of the services offered. That said, when processing personal information by a processor, the controller (being the CITC licensed service provider) must assure compliance and security of such data. Thus, an agreement must be entered into between the controller and processor.

## 9 Marketing

**9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).**

As per paragraph B of Article 5 (2) of the E-Commerce Law and its Implementing Regulations, service providers are restricted from using processed data for the purpose of advertainment and marketing without obtaining the explicit consent of the concerned individual.

**9.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?**

As mentioned above, these restrictions are applicable to business-to-consumer marketing.

**9.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).**

The regulations do not address this.

**9.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?**

The restrictions as mentioned in question 9.1 apply to all service providers offering services in the Kingdom, pursuant to Article 2 of the E-Commerce Law. Therefore, the E-Commerce Law applies to service providers residing in another jurisdiction but offering services in the Kingdom.

**9.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?**

The Ministry of Commerce shall oversee any breach of e-commerce marketing and advertisement activities.

**9.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?**

The current regulations do not discuss this.

**9.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?**

Article 18 of the E-Commerce Law sets out a maximum penalty of SAR 1 million for a violation of the Law and its Implementing Regulations. The penalty may also include a warning to the violator, cessation of the e-commerce activity, or blocking of the violated e-store, as further explained in question 15.4 below.

## 10 Cookies

**10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).**

This is not applicable.

**10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?**

This is not applicable.

**10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?**

The CITC oversees and assesses the risk associated with data privacy by CITC licensed service providers. This includes collection of sensitive data and the effect on data subjects when collected using cookies.

**10.4 What are the maximum penalties for breaches of applicable cookie restrictions?**

The current regulations do not identify a specific penalty for breaches of cookie restrictions.

## 11 Restrictions on International Data Transfers

**11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.**

With the absence of a conclusive data protection regulation, at this time there are no specific rules for data transfer to third countries or international organisations. Article 5 (4) of the General Principles stipulates that service providers shall adhere to processing users' data within the Kingdom. Such data shall not be transferred abroad unless approved by the CITC. As such, where service providers wish to transfer data to third countries or international organisations (which do not have local presence), such transfer shall be subject to the CITC's approval.

**11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).**

As mentioned at question 11.1, according to the General Principles, service providers should adhere to processing users' data within the Kingdom; however, if data is transferred to a different jurisdiction, the CITC's approval will be provided on a case-by-case basis.

**11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.**

As per Article 5 (4) of the General Principles, service providers shall adhere to processing users' data within the Kingdom, and such data shall not be transferred abroad without the prior approval of the CITC.

**11.4 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?**

This is not applicable.

**11.5 What guidance (if any) has/have the data protection authority(ies) issued in relation to the European Commission's revised Standard Contractual Clauses?**

This is not applicable.

## 12 Whistle-blower Hotlines

**12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?**

This is not applicable.

**12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?**

This is not applicable.

## 13 CCTV

**13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?**

This is not applicable.

**13.2 Are there limits on the purposes for which CCTV data may be used?**

This is not applicable.

## 14 Employee Monitoring

**14.1 What types of employee monitoring are permitted (if any), and in what circumstances?**

This is not applicable.

**14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.**

This is not applicable.

**14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?**

This is not applicable.

## 15 Data Security and Data Breach

**15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?**

Pursuant to Article 5 (2) of the E-Commerce Law, service providers are obligated to take all necessary measures to ensure the protection of user data. Service providers are also expected to maintain the data required for a specific purpose and not to utilise it in a way that differs from the purpose for which said data is processed. In the event that the processed data has been subject to unauthorised access or leakage, such incident must be reported to the Ministry of Commerce, and the service provider shall be responsible before the relevant user for such penetration.

Furthermore, Articles 5 (1) and 5 (2) of the General Principles obligate service providers to develop and implement programmes and procedures related to the preservation of personal data that are subject to the approval of the CITC. As such, the CITC is granted supervisory authority to ensure the level of compliance carried out by the service providers with respect to their obligations as set forth in the General Principles.

**15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

As mentioned above, pursuant to Article 5 (2) of E-Commerce Law, any data leakage or unauthorised access to data must be reported to the Ministry of Commerce.

**15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

The CITC requires service providers to notify the commission of any breach to data privacy.

**15.4 What are the maximum penalties for data security breaches?**

Article 18 of the E-Commerce Law lists a number of penalties that may be issued against an entity violating the law. These penalties are as follows:

1. a warning;
2. a fine not exceeding SAR 1 million;
3. a permanent suspension of carrying out its e-commerce activities; and
4. blocking the e-shop (temporarily or permanently) as per the competent court's discretion.

Additionally, Article 22 of the E-Commerce Law obligates the competent courts to settle disputes and claims arising from the implementation of said laws. Further, Article 27 of the E-Transactions Law provides that should a person incur damage due to violations attributable to said law, such individual has the right to claim damages before the competent authority. Thus, the legal remedies will depend on the severity of the harm and the ruling issued by the competent authority.

## 16 Enforcement and Sanctions

**16.1 Describe the enforcement powers of the data protection authority(ies).**

(a) **Investigative Powers**: awaiting publication of the regulation and guideline.
(b) **Corrective Powers**: awaiting publication of the regulation and guideline.
(c) **Authorisation and Advisory Powers**: awaiting publication of the regulation and guideline.
(d) **Imposition of administrative fines for infringements of specified GDPR provisions**: awaiting publication of the regulation and guideline.
(e) **Non-compliance with a data protection authority**: awaiting publication of the regulation and guideline.

**16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?**

This is not applicable.

**16.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.**

This is not applicable.

**16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?**

This is not applicable.

## 17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

**17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?**

This is not applicable.

**17.2 What guidance has/have the data protection authority(ies) issued?**

This is not applicable.

## 18 Trends and Developments

**18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.**

This is not applicable.

**18.2 What "hot topics" are currently a focus for the data protection regulator?**

There are currently no specific topics of focus for data protection regulators. However, we anticipate that the data protection regulation, once issued, will adopt similar protections to data subjects as those under the GDPR.

**Suhaib Hammad** joined Hammad and Al-Mehdar Law Firm in 2009. He earned his LL.B. from IIU Malaysia and his LL.M. from the University of Miami, specialising in International Business Law.
As a Partner, Suhaib leads the Commercial and Intellectual Property practice, focusing on ICT, TMT and Life Sciences. In addition, Suhaib was placed on secondment with the corporate and commercial team at Simmons & Simmons in their Dubai and London offices, and has worked on leading cross-border transactions. His experience includes advising major international telecoms and healthcare companies on Saudi regulations in relation to formation and operation. Suhaib was also awarded a Client Choice Award by *Lexology* for the year 2019. The firm was recognised as the best Mergers & Acquisitions law firm for the years 2017 and 2018 by the IFN Law Awards, and has been honourably mentioned as a Tier 1 Firm in *The Legal 500 2017* for Banking & Finance Transactions.

**Hammad and Al-Mehdar Law Firm**
Level 12, Office 1209
King Road Tower
King Abdulaziz Road
Jeddah
Saudi Arabia

Tel: +966 920 004 626
Email: suhaib.hammad@hmco.com.sa
URL: www.hmco.com.sa

Hammad and Al-Mehdar Law Firm was founded in 1983 in Jeddah, Saudi Arabia, and has grown to become a prominent private practice Saudi firm in the Kingdom and the GCC. The law firm boasts a leading local presence supported by international capabilities.
Hammad and Al-Mehdar provides a full suite of business and corporate legal services in all major areas of Saudi law, working on cutting-edge, complex and high-value transactions and disputes.
Headquartered in Jeddah, Hammad and Al-Mehdar's growth story is one of trade, innovation and technology in the Kingdom's private sector. Hammad and Al-Mehdar maintains a strong specialisation in servicing privately held businesses, with unrivalled expertise in business and transaction structuring, private construction works, commercial, intellectual property, corporate governance, and regulatory advisory services.

**www.hmco.com.sa**

HAMMAD & AL-MEHDAR
LAW FIRM

# Senegal



LPS L@W

Léon Patrice SARR

## 1 Relevant Legislation and Competent Authorities

### 1.1 What is the principal data protection legislation?

The principal data protection legislation is Law no. 2008-12 dated 25 January 2008 relating to the protection of personal data (Data Protection Act) ("DPA"), decree no. 2008-721 dated 30 June 2008 relating to the application of the DPA, and Law no. 2016-29 dated 8 November 2016 modifying the penal code. The DPA and its application decree provide the conditions relating to data processing, the rights of Data Subjects and the obligations of Data Controllers. The DPA creates the Senegalese Data Protection Authority (*Commission de Protection des Données Personnelles*) ("CDP") Law no. 2016-29 dated 8 November 2016 modifying the penal code, which provides criminal offences relating to data processing and the applicable sanctions.

### 1.2 Is there any other general legislation that impacts data protection?

There is no other general legislation that impacts data protection.

### 1.3 Is there any sector-specific legislation that impacts data protection?

There is no sector-specific legislation that impacts data protection.

### 1.4 What authority(ies) are responsible for data protection?

The authority responsible for data protection is the CDP.

## 2 Definitions

### 2.1 Please provide the key definitions used in the relevant legislation:

- "**Personal Data**"
  "Personal Data" means all data relating to an identified or identifiable individual with reference to an identification number or one, or many, characteristics of his physical, physiological, genetic, psychical, cultural, social or economic identity.
- "**Processing**"
  "Processing" of personal data (or "Data Processing") means any operation or set of operations in relation to such data, especially their collection, exploitation, registration, organisation, storage, adaptation, modification, retrieval, backup, copying, consultation, utilisation, disclosure by transmission, dissemination or otherwise making available, alignment, locking, encryption, erasure or destruction.
- "**Controller**"
  "Controller" means all persons who (either alone, jointly or in common with other persons) take the decision to collect and process personal data and determine the purposes of the processing.
- "**Processor**"
  "Processor" means all persons who (either alone, jointly or in common with other persons) collect, exploit, register, organise, store, adapt, modify, retrieve, back up, copy, consult, use or disclose data by transmission, disseminate or otherwise make available, align, lock, encrypt, erase or destroy.
- "**Data Subject**"
  "Data Subject" means all individual persons whose personal data are processed.
- "**Sensitive Personal Data**"
  "Sensitive Personal Data" means data relating to: religious, philosophical or political opinions or union activities; sex life; race; health; social measures and prosecutions; and criminal and administrative sanctions.
- "**Data Breach**"
  "Data Breach" means any operation or attempted operation involving such data, especially their interception, misappropriation, damage, deletion, erasure, alteration or counterfeiting by an unauthorised production, use, backup or transfer process.

## 3 Territorial Scope

### 3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

Yes, if the business' means of processing are located in Senegal, unless they are for transit only.

## 4 Key Principles

### 4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  Under Article 35 of the DPA, Data Controllers must inform the Data Subjects about the processing and personal data processed.
- **Lawful basis for processing**
  Under Article 34 of the DPA, personal data must be processed lawfully and fairly.
- **Purpose limitation**
  Under Article 35 of the DPA, personal data may only be obtained for specific, explicit and legitimate purposes, and cannot be further processed in any manner incompatible with those purposes.
- **Data minimisation**
  Under Article 35 of the DPA, personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and further processed.
- **Proportionality**
  Refer to "Data minimisation".
- **Retention**
  Under Article 35 of the DPA, personal data must not be retained for longer than is necessary for the purposes for which they are collected and further processed.
- **Confidentiality**
  Under Article 35 of the DPA, the Data Controller must ensure confidentiality and security of the processing.
- **Legitimacy**
  Under Article 33 of the DPA, the processing of personal data is legitimate if the Data Subject consents to the processing. The consent must be express, unequivocal, free and specific.
  However, under Article 33 of the DPA, processing can be justified without the Data Subject's consent on any of the following grounds: compliance with any legal obligation to which the Data Controller is subject; performance of a public service undertaking that has been entrusted to the Data Controller or the data recipient; the processing relates to the performance of a contract to which the Data Subject is a party, or of pre-contractual measures requested by him; and processing the data is subject to the interests and fundamental rights and liberties of the Data Subject.

## 5 Individual Rights

### 5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**
  Pursuant to Article 62 of the DPA, Data Subjects have a right of access and they can obtain the following from the Data Controller:
  - Information which they are entitled to know and which will allow them to contest the processing.
  - Confirmation of whether their personal data forms part of the processing.
  - A copy of their personal data (in an accessible form), as well as any available information on the data's origin.

  Information relating to the: purposes of the processing; categories of processed data; recipients or categories of recipients to whom the data are disclosed; and transfer of personal data outside the country.
  The right of access is limited when the processing involves state security, defence or public safety.
- **Right to rectification of errors**
  Pursuant to Article 69 of the DPA, Data Subjects can request that the Data Controller rectify or delete their personal data if they are inaccurate, incomplete, unclear or expired, or if the collection, usage, disclosure or retention of the data is prohibited.
- **Right to deletion/right to be forgotten**
  Regarding the right to deletion, please refer to "Right to rectification of errors".
  There is no "right to be forgotten" in current Senegalese law.
- **Right to object to processing**
  Pursuant to Article 63 of the DPA, Data Subjects have the right to object to the processing on legitimate grounds, unless the processing satisfies a legal obligation.
- **Right to restrict processing**
  Please refer to "Right to object to processing".
- **Right to data portability**
  There is no such right in Senegalese law.
- **Right to withdraw consent**
  Pursuant to Article 33 of the DPA, data processing requires the Data Subject's prior consent. However, his consent is not required in the following instances:
  - If required by the law.
  - To fulfil a general interest mission or required by the public authority.
  - For the execution of an agreement, if the processor is party to the contract.
  - For fundamental freedoms and personal interest safeguarding.
- **Right to object to marketing**
  Data Subjects have the right to object, free of charge, to the processing of their Personal Data for direct marketing.
- **Right to complain to the relevant data protection authority(ies)**
  Data Subjects can complain to the CDP at any time the processing of their Personal Data does not comply with the DPA provisions.

## 6 Registration Formalities and Prior Approval

### 6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

Under Article 18 of the DPA, businesses must notify the CDP in respect of their processing activities, except in the following cases:

- Non-profit processing for religious, philosophical or political associations, or trade unions (when the data correspond to the purpose of the association or trade union, concern only their members and are not disclosed to third parties).
- Processing for the sole purpose of keeping a register; by law, this is intended exclusively to provide public information and is open to consultation for any person with a legitimate interest.

**6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?**

The notification/registration must be specific.

**6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?**

Notifications are made per processing purpose.

**6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?**

Pursuant to Article 22 of the DPA, the Data Controller must notify the data protection authority regardless of whether he is a local or foreign legal entity. If the Data Controller is not established in Senegal, he must communicate to the data protection authority his legal representative in Senegal.

**6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?**

The declaration must include the following:

- Identity and address of the Data Controller or his representative.
- Purpose(s) of the processing and the description of its general functions.
- Possible interconnections between databases.
- Personal data processed and categories of persons concerned in its processing.
- Time period for which the data will be kept.
- Department or person(s) in charge of data processing.
- Recipient(s) or categories of recipients of the processed data.
- Persons or departments before which the right of access is exercised.
- Measures taken to ensure the security of the processing.
- Identity and address of the data processor.

**6.6 What are the sanctions for failure to register/notify where required?**

Sanctions for failure to register/notify are:

- Imprisonment for a period of between one and seven years.
- Fines of between XOF 500,000 and 10 million.

The judge can choose one of the sanctions listed above or a combination of them.

**6.7 What is the fee per registration/notification (if applicable)?**

There is no fee.

**6.8 How frequently must registrations/notifications be renewed (if applicable)?**

Notifications must be renewed any time the information provided changes.

**6.9 Is any prior approval required from the data protection regulator?**

Under Article 20 of the DPA, prior approval from the CDP is required for processing of:

- Genetic data.
- Data relating to offences, convictions or security measures.
- Data that involve an interconnection of files.
- Data that include a national identification number.
- Biometric data.
- Data that are of public interest, particularly for historical, statistical or scientific purposes.

Authorisation is not required in the following cases:

- Data processing for private purposes only.
- Temporary data copies for transmission, network access and automatic storage purposes, provided they are made to improve network user access.
- Data processing by non-profit organisations for religious, philosophic, political or union purposes only.
- Data processing for public register purposes.

**6.10 Can the registration/notification be completed online?**

Notifications cannot be completed online; however, they can be sent online.

**6.11 Is there a publicly available list of completed registrations/notifications?**

The list of completed notifications is available on the CDP website: http://www.cdp.sn/repertoire-des-declarations.

**6.12 How long does a typical registration/notification process take?**

A typical registration/notification process takes two months, unless extended (once) by a reasoned decision from the CDP.

## 7 Appointment of a Data Protection Officer

**7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.**

There is no provision relating to the appointment of a Data Protection Officer. However, the DPA provides that the person or department where the access right is exercised must be communicated to the CDP.

**7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?**

There are no sanctions.

**7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?**

There is no particular protection for Data Protection Officers.

**7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?**

There are no legal limitations.

**7.5 Please describe any specific qualifications for the Data Protection Officer required by law.**

There are no specific qualifications required by law.

**7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?**

There is no provision on the responsibilities of Data Protection Officers in the DPA.

**7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?**

The DPA does not provide that the Data Protection Officer must be notified to the CDP. However, under Article 22 of the DPA, the person or department where the access right is exercised must be communicated to the CDP.

**7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?**

The DPA does not provide that Data Protection Officers must be named in a public-facing privacy notice or equivalent document.

## 8 Appointment of Processors

**8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?**

The business shall sign a subcontract agreement with the processor.

**8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?**

Under the provisions of Article 39 of the DPA, the subcontract agreement must be written and must stipulate that the subcontractor must only process personal data in accordance with the processor's instructions. He must also take every necessary measure to ensure the data's security and safety.

## 9 Marketing

**9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).**

The sending of marketing communications is forbidden pursuant to Article 47 of the DPA and Article 16 of the Senegalese Electronic Transactions Law unless the recipient agrees to it. However, there are two exceptions where prior approval is not required:

- The recipient's information was collected directly from him, in accordance with the provisions of the DPA.
- The recipient is already a customer of the company, the marketing messages relate to products or services that are similar to those previously provided, and the recipient is given the possibility of objecting to all messages sent to him.

**9.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?**

Article 47 of the DPA does not specify this. Consequently, the restrictions apply to both business-to-consumer and business-to-business relationships.

**9.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).**

Article 47 of the DPA does not distinguish the means used.

**9.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?**

Yes, the restrictions above apply to marketing sent from other jurisdictions.

**9.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?**

Yes. Since 2014, the CDP has sent several warnings and notices to different companies for breaches of marketing restrictions. For example:

- EXPRESSO TELECOM was sent a warning on 3 April 2014 for unrequested advertisement.
- GEGINUS was sent a warning on 20 April 2014 for failure to respect data protection law.
- HELLO FOOD SENEGAL was sent a warning on 15 May 2015 for failure to respect data protection law.
- DIGITAL VIRGO was sent a warning on 31 July 2015 for failure to respect the legal prospection terms.
- EXPRESSO TELECOM was summoned on 20 October 2017 for failure to respect data protection law.
- CBAO ATTIJARIWAFA BANK was summoned on 20 October 2017 for failure to respect data protection law.

**9.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?**

Pursuant to Article 47 of the DPA, it is unlawful to purchase marketing lists from third parties.

**9.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?**

According to Article 431-20 of the Senegalese Criminal Law, the maximum penalties for sending marketing communications in breach of applicable restrictions are seven years' imprisonment or an XOF 1 million fine, or both.

## 10 Cookies

**10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).**

There is no restriction on the use of cookies. However, the CDP requires that the Data Subject is informed of the use of cookies and to collect his consent.

**10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?**

This is not applicable in Senegal.

**10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?**

We are not aware of any enforcement action in relation to cookies.

**10.4 What are the maximum penalties for breaches of applicable cookie restrictions?**

We are not aware of any penalty.

## 11 Restrictions on International Data Transfers

**11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.**

Pursuant to Article 49 of the DPA, transfer of personal data to another country is prohibited unless the receiving country provides sufficient protection for the Data Subject's private life, liberties and fundamental rights.

**11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).**

The transfer of personal data abroad is possible only if the recipient country offers a sufficient level of protection of privacy, liberty and fundamental rights to Data Subjects. Before transferring personal data, the company must inform the CDP. The information must include:

- The name and address of the data sender.
- The name and address of the data recipient.
- The full data file and description.
- The type of personal data transferred.
- The number of persons concerned.
- The data processing purpose.
- The transfer method and frequency.
- The first transfer date.

A transfer to a country not offering a sufficient level of protection is possible if the transfer is timely and non-massive, if the Data Subject agrees to it or if the transfer is necessary to:

- protect the life of the Data Subject;
- protect the public interest;
- comply with obligations allowing the acknowledgment, exercise or defence of a legal right in court; and
- perform an agreement between the Data Subject and the Data Processor or take precontractual measures upon the request of the Data Subject.

The CDP can allow a transfer to a country that does not offer a sufficient level of protection, based on a reasoned request, if the Data Processor offers sufficient guarantees of privacy, liberty and fundamental rights to Data Subjects.

**11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.**

The transfer of personal data to a country that provides sufficient protection requires notification to the CDP before the transfer. The Data Controller fills in and files the notification form. All changes in the information notified must be declared to the CDP within 15 working days. The CDP intended to establish a list of the countries that offer sufficient protection. However, so far, the list does not exist.

The transfer of personal data to a country that does not provide sufficient protection requires prior authorisation from the CDP. The Data Controller must fill in and file the authorisation request form. The CDP issues the decision within two months, extendable once. The Data Controller must file another authorisation request if any change affects the information provided to the CDP.

**11.4 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?**

We are not aware of any guidance issued by the CDP following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18).

**11.5 What guidance (if any) has/have the data protection authority(ies) issued in relation to the European Commission's revised Standard Contractual Clauses?**

We are not aware of any guidance issued by the CDP in relation to the European Commission's (draft) revised Standard Contractual Clauses.

## 12 Whistle-blower Hotlines

**12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?**

To the best of our knowledge, there is no legal provision or binding guidance issued by the CDP on corporate whistle-blower hotlines.

**12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?**

This is not applicable in Senegal.

## 13 CCTV

**13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?**

The CDP issued deliberation no. 2015-00186/CDP dated 8 January 2016 relating to CCTV surveillance, and deliberation no. 2016-00238 dated 11 November 2016 relating to the rules governing CCTV installation and exploitation in workplaces, which state that the use of CCTV requires a separate notification to the CDP. However, data collected and stored abroad require prior authorisation from the CDP.

**13.2 Are there limits on the purposes for which CCTV data may be used?**

A CCTV system may be used only:

- For assets and personal security purposes when used by individuals. In such case, the CCTV system must only cover the house perimeter.
- For security and infringement prevention or recognition in public areas – the reasons for which it is used by public authorities.
- For business premises' security and access, or the monitoring of employees' movements, when used by private corporations.

Any other use requires CDP approval.

## 14 Employee Monitoring

**14.1 What types of employee monitoring are permitted (if any), and in what circumstances?**

Pursuant to deliberation no. 2016-00238, employee monitoring is allowed for employee and asset security. A CCTV system cannot be used for employee monitoring only.

A CCTV system can be installed in the following places:

- Premises' entrances and exits.
- Corridors and hallways.
- Emergency exits.
- Parking lots.
- Waiting rooms.
- Warehouses.
- Cash registers.

CCTV cannot be installed in the following places:

- Locker rooms.
- Break rooms.
- Staff representative premises.

**14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.**

In deliberation no. 2015-00165/CDP dated 6 November 2016, the CDP stated that employers may control and limit the use of the internet or professional devices for performance or security purposes. It includes for employers the right to have access to professional emails and websites visited. However, employers must respect employees' intimacy and privacy, even in workplaces and during working hours. This means that employers cannot access private messages even if the personal use of professional devices is prohibited. Employers can access employees' private emails only if justified by the protection of a superior interest and in the presence of a bailiff or the employee.

In deliberation no. 2016-00238 dated 11 November 2016, relating to the rules governing CCTV installation and exploitation in workplaces, the CDP stated that employers may carry out CCTV monitoring for safety, management of staff movement and access control purposes. Any other purpose is subject to the CDP's discretion.

**14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?**

In deliberation no. 2016-00238 dated 11 November 2016, the CDP stated that employee representatives must be informed and consulted prior to CCTV surveillance.

## 15 Data Security and Data Breach

**15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?**

Pursuant to Article 71 of the DPA, Data Controllers are required to ensure the security of personal data. They must prevent the data's alteration and damage, or access by non-authorised third parties. Additionally, Data Controllers must make sure that:

- Persons with access to the system can only access the data that they are allowed to access.
- The identity and interest of any third-party recipients of the data can be verified.
- The identity of persons who have access to the system (to view or add data) can be verified.
- Unauthorised persons cannot access the place and equipment used for the data processing.
- Unauthorised persons cannot read, copy, modify, destroy or move data.
- All data entered onto the system are authorised.
- The data will not be read, copied, modified or deleted without authorisation during the transport or communication of the data.
- The data are backed up with security copies.
- The data are renewed and converted in order to preserve them.

**15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

There is no legal requirement to report data breaches to the CDP.

**15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

There is no legal requirement to report data breaches to individuals.

**15.4 What are the maximum penalties for data security breaches?**

The maximum criminal penalty for security breaches is imprisonment for one to seven years or a fine of between XOF 500,000 and XOF 10 million, or both. In addition, the CDP can impose an administrative fine of between XOF 1 million and XOF 100 million.

## 16 Enforcement and Sanctions

**16.1 Describe the enforcement powers of the data protection authority(ies).**

(a) **Investigative powers**:
The CDP can conduct three types of investigation:
*On-site inspections*
In this case, the CDP may have access to any materials (servers, computers, applications, etc.) and any place (offices, buildings) in which personal data are processed.
*Documentary inspections*
These inspections allow the CDP to obtain disclosure of documents or files upon written request.
*Hearing inspections*
These inspections consist of interrogation in their offices or summoning representatives of Data Controllers in order to obtain any necessary information.

(b) **Corrective powers**:
We are not aware of any corrective power.

(c) **Authorisation and advisory powers**:
The CDP authorises the processing of certain categories of data, the interconnection of data and, under certain conditions, cross-border transfers of personal data.
The CDP informs Data Controllers and Data Subjects of their rights and obligations and advises individuals and legal entities processing personal data or carrying out tests or experiments likely to lead to such processing.
The CDP communicates to the Government any suggestions that may simplify and improve the legislative and regulatory framework of data processing.

(d) **Imposition of administrative fines for infringements of specified GDPR provisions**:
The CDP has no power to impose administrative fines for infringement of specified GDPR provisions.
The CDP can impose an administrative fine between XOF 1 million and XOF 100 million in case of infringement of the DPA.

(e) **Non-compliance with a data protection authority**:
Non-compliance with the CDP can lead to the following sanctions:
- a warning;
- an injunction to put an end to defaults within the time limit set by the Commission; or
- a provisional withdrawal of the authorisation granted for a period of three months at the expiry of which the withdrawal becomes final.

In case of urgency, the CDP can:
- interrupt a processing for a duration that cannot exceed three months;
- lock certain kinds of data for a duration that cannot exceed three months; or
- prohibit, provisionally or definitively, data processing that does not comply with the DPA.

**16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?**

Pursuant to Article 31 of the DPA, the CDP has the power to issue a temporary or permanent ban. The ban does not require a court order.

**16.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.**

After its installation in December 2013, the CDP published a press release inviting Data Controllers to notify it of the processing of their data. The CDP also sent letters directly to certain companies for the same purpose. The companies who failed to notify or to provide the additional information requested by the CDP received either a notice or a warning. The CDP also sent several notices and warnings to different companies for breach of the restrictions on the sending of marketing communications. To the best of our knowledge, there has been no fine imposed so far.

On 3 April 2014, EXPRESSO received a warning for failure to notify its processing and for failure to respect the restrictions on the sending of marketing communications.

On 30 April 2014, SONATEL received a notice for failure to notify the database relating to the sending of marketing communications, failure to respect the restrictions on the sending of marketing communications, and failure on security and confidentiality measures.

On 30 April 2014, TIGO received a notice for failure to notify its processing and failure to respect the restrictions on the sending of marketing communications.

On 15 May 2015, DIGITAL VIRGO received a warning for failure to request the consent of Data Subjects and their rights of information and objection, and failure to respect the restrictions on the sending of marketing communications.

On 31 July 2015, HELLO FOOD SENEGAL received a warning for failure to notify the processing of personal data, failure to respect the fundamental principles of data protection, failure to respect the rights of Data Subjects, and failure to respect the restrictions on the sending of marketing communications.

On 6 November 2015, AFRIQUE PETROLE received a warning for monitoring employees' private emails.

**16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?**

The CDP does not exercise its powers against businesses established in other jurisdictions.

## 17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

**17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?**

We have no information on how businesses respond to foreign e-discovery requests or requests for disclosure from foreign law enforcement agencies. This information is not public.

**17.2 What guidance has/have the data protection authority(ies) issued?**

The CDP has issued no guidance on this topic.

## 18 Trends and Developments

**18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.**

There has been no emergence of any enforcement trends during the previous 12 months. The CDP has so far opted to send notices and warnings because Data Controllers generally react positively by complying with the DPA provisions.

**18.2 What "hot topics" are currently a focus for the data protection regulator?**

The current "hot topic" with the CDP is the creation in Senegalese law of a right to be forgotten. The CDP authorities agree and admit that every Senegalese citizen should have the right to obtain the withdrawal of published compromising or personal information. Unfortunately, as of yet, no legal measure has been taken to this end.

**Léon Patrice SARR** is the Founding Partner of LPS L@w. His experience with various renowned Senegalese and foreign law firms and his ability to work in several branches of law give him an international stature. His prompt capacity to understand and his innovative solutions allow him to successfully complete very complex cases.

**LPS L@W**
Cité keur Gorgui, lor n°40, 6th Floor
Dakar
Senegal

Tel: +221 33 848 79 88
Email: lp.sarr@lps-law.com
URL: www.lps-law.com

# Singapore

Drew & Napier LLC

Lim Chong Kin

## 1 Relevant Legislation and Competent Authorities

### 1.1 What is the principal data protection legislation?

The Personal Data Protection Act 2012 (No. 26 of 2012) ("**PDPA**") is the principal data protection legislation in Singapore. The PDPA establishes a general data protection law which applies to all private sector organisations.

The PDPA has recently undergone its first comprehensive review since its enactment, and the amendments are set out in the Personal Data Protection (Amendment) Act 2020 ("**Amendment Act**"). The Amendment Act, which was passed in Parliament on 2 November 2020, sets out extensive amendments which have mostly come into effect on 1 February 2021.

Parts III to VIB of the PDPA set out obligations of organisations in respect of the collection, use, disclosure, access, correction, care, protection, retention, and transfer of personal data (collectively, "**Data Protection Provisions**"); while Part IX of the PDPA sets out provisions pertaining to Singapore's national Do Not Call ("**DNC**") Registry and the obligations of organisations in relation to sending marketing messages to Singapore telephone numbers ("**DNC Provisions**").

Other regulations issued under the PDPA are:

- the Personal Data Protection Regulations 2021 ("**PDP Regulations**"), which set out the requirements for transfers of personal data out of Singapore; the form, manner and procedures for requests for access to or correction of personal data; and persons who may exercise rights in relation to disclosure of personal data of deceased individuals;
- the Personal Data Protection (Notification of Data Breaches) Regulations 2021;
- the Personal Data Protection (Composition of Offences) Regulations 2021;
- the Personal Data Protection (Do Not Call Registry) Regulations 2013;
- the Personal Data Protection (Enforcement) Regulations 2021; and
- the Personal Data Protection (Appeal) Regulations 2021.

In addition, the Personal Data Protection Commission ("**PDPC**") has issued a number of advisory guidelines which provide greater clarity on the interpretation of the PDPA.

### 1.2 Is there any other general legislation that impacts data protection?

The Computer Misuse Act (Cap. 50A) sets out a number of offences which include the unauthorised access or modification of computer material, as well as the unauthorised use or interception of computer services.

The Cybersecurity Act 2018 (No. 9 of 2018) requires owners and operators of Critical Information Infrastructure to comply with cybersecurity policies and standards, conduct audits and risk assessments, and implement incident reporting measures.

For completeness, the Spam Control Act (Cap. 311A) ("**SCA**") regulates the bulk sending of unsolicited commercial electronic messages to email addresses or mobile telephone numbers, complementing the DNC Provisions of the PDPA.

### 1.3 Is there any sector-specific legislation that impacts data protection?

Yes, a number of other regulations and pieces of legislation in Singapore contain certain sector-specific data protection requirements. For example:

- the Banking Act (Cap. 19) ("**Banking Act**") contains a number of banking secrecy provisions which govern customer information obtained by banks;
- the Telecoms Competition Code issued under the Telecommunications Act (Cap. 323) contains provisions governing the use of end-user service information by telecoms licensees; and
- the Private Hospitals and Medical Clinics Act (Cap. 248) and the licensing terms and conditions issued thereunder contain provisions addressing the confidentiality of medical information and the retention of medical records.

With regard to the financial sector, the Monetary Authority of Singapore ("**MAS**") is empowered under the Monetary Authority of Singapore Act (Cap. 186) and other sectoral legislation to issue directives and notices. Examples of MAS-issued regulatory instruments which are relevant to data protection include the Notices on Cyber Hygiene, Notices and Guidelines on Technology Risk Management, and the Guidelines on Outsourcing.

In this regard, Section 4(6) of the PDPA provides that the general data protection framework does not affect any right or obligation under the law, and that in the event of any inconsistency, the provisions of other written laws will prevail.

The PDPC has also developed sector-specific advisory guidelines for the telecommunications sector, the real estate agency sector, the education sector, the healthcare sector, the social services sector and transport services for hire (specifically in relation to in-vehicle recordings).

In addition, the PDPC has provided comments and suggestions to industry-led guidelines on the PDPA that were developed by industry associations such as:

- the Life Insurance Association Singapore ("**LIA**") Code of Practice for Life Insurers on the Singapore Personal Data Protection Act; and
- the LIA Code of Conduct for Tied Agents of Life Insurers on the Singapore Personal Data Protection Act.

### 1.4 What authority(ies) are responsible for data protection?

The PDPC is responsible for administering and enforcing the PDPA. The PDPC is under the purview of the Ministry of Communications and Information ("**MCI**"), and is part of the merged info-communications and media regulator, the Info-communications Media Development Authority of Singapore ("**IMDA**") (previously the Info-communications Development Authority of Singapore and the Media Development Authority of Singapore).

Sector-specific data protection obligations are separately enforced by the relevant sectoral regulators. For example, the MAS enforces the banking secrecy provisions under the Banking Act and other sectoral legislation and regulatory instruments governing other types of financial institutions.

## 2 Definitions

### 2.1 Please provide the key definitions used in the relevant legislation:

- "**Personal Data**"
  "Personal data" is defined under the PDPA as data, whether true or not, about an individual who can be identified: (a) from that data; or (b) from that data and other information to which the organisation is likely to have access.
  All formats of personal data are covered under the PDPA, whether electronic or non-electronic, and regardless of the degree of sensitivity.
- "**Processing**"
  Under the PDPA, "processing", in relation to personal data, means the carrying out of any operation or set of operations in relation to the personal data, and includes any of the following:
  (a) recording;
  (b) holding;
  (c) organisation, adaptation or alteration;
  (d) retrieval;
  (e) combination;
  (f) transmission; and
  (g) erasure or destruction.
- "**Controller**"
  The PDPA does not use the term "controller", but instead refers to an "organisation". An "organisation" is defined as any individual, company, association or body of persons, corporate or unincorporated, whether or not: (a) formed or recognised under the law of Singapore; or (b) resident, or having an office or a place of business, in Singapore.
- "**Processor**"
  Similarly, the PDPA does not use the term "processor", but instead refers to a "data intermediary", which is defined as an organisation which processes personal data on behalf of another organisation but does not include an employee of that other organisation.
  The PDPA provides that a data intermediary that processes personal data on behalf of and for the purposes of another organisation pursuant to a contract which is evidenced or made in writing will only be subject to (i) the Protection Obligation, (ii) the Retention Limitation Obligation (as defined below), and (iii) the requirement to notify the data controller where the data intermediary has reason to believe that a data breach has occurred in relation to personal data that it is processing on the data controller's behalf.
- "**Data Subject**"
  The PDPA does not use the term "data subject", but instead refers generally to an "individual", whose personal data is collected, used, disclosed, or otherwise processed by organisations. An "individual" is defined to mean a natural person, whether living or deceased.
- "**Sensitive Personal Data**"
  The PDPA does not expressly distinguish between specific categories of personal data. The term "sensitive personal data" is therefore not defined.
  However, as a number of the Data Protection Provisions adopt a standard of reasonableness, the sensitivity of the personal data in question could, in practice, affect the extent of the data protection obligations an organisation is subject to. The PDPC has taken the position in several enforcement decisions that a higher standard of protection is required for more sensitive personal data, which includes insurance, medical and financial data (see in *Re Aviva Ltd* [2017] SGPDPC 14).
  In this regard, the PDPC's Advisory Guidelines on Enforcement for Data Protection Provisions ("**Enforcement Guidelines**") provide that, if an organisation which has breached a Data Protection Provision is in the business of handling large volumes of sensitive personal data, the disclosure of which may cause exceptional damage, injury, or hardship to a person (such as medical or financial data), but failed to put in place adequate safeguards proportional to the harm that might be caused by disclosure of such personal data, the PDPC may also consider this to be an aggravating factor in calculating the level of the financial penalty to be imposed on the organisation.
- "**Data Breach**"
  "Data breach" is defined in Part VIA of the PDPA to mean: (a) the unauthorised access, collection, use, disclosure, copying, modification or disposal of personal data; or (b) the loss of any storage medium or device on which personal data is stored in circumstances where the unauthorised access, collection, use, disclosure, copying, modification or disposal of the personal data is likely to occur.
- **Other key definitions**
  "Business contact information" is defined as an individual's name, position name or title, business telephone number, business address, business electronic mail address or business fax number and any other similar information about the individual, not provided by the individual solely for his personal purposes.
  Organisations are not required to obtain consent before collecting, using or disclosing any business contact information, or to comply with any other obligation in the Data Protection Provisions in relation to business contact information.

## 3 Territorial Scope

### 3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The PDPA applies to all organisations which are not a public agency, whether or not formed or recognised under the laws of

Singapore, or resident or having an office or a place of business in Singapore.

According to the PDPC's Advisory Guidelines on Key Concepts in the PDPA ("**Key Concepts Guidelines**"), the Data Protection Provisions apply to organisations carrying out activities involving personal data in Singapore. Thus, where personal data is collected overseas and subsequently transferred into Singapore, the Data Protection Provisions will apply in respect of the activities involving the personal data in Singapore.

## 4 Key Principles

### 4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  Section 20 of the PDPA provides that an organisation must notify an individual of the purpose(s) for which it intends to collect, use, or disclose his personal data, on or before such collection, use, or disclosure ("**Notification Obligation**").
  More generally, Sections 11 and 12 of the PDPA require an organisation to develop and implement policies and practices that are necessary for the organisation to meet its obligations under the PDPA, communicate such policies and practices to its employees, and make information about its policies and procedures publicly available ("**Accountability Obligation**"). Accountability under the PDPA requires organisations to undertake measures in order to ensure that they meet their obligations under the PDPA and, importantly, demonstrate that they can do so when required. The Accountability Obligation also requires an organisation to appoint a Data Protection Officer (see section 7 below).
- **Lawful basis for processing**
  Sections 13 to 17 of the PDPA generally require that an organisation obtain the consent of an individual before collecting, using, or disclosing his personal data for a purpose ("**Consent Obligation**"), unless an exception in the First or Second Schedule to the PDPA applies. Such consent from an individual must be validly obtained and may be either expressly given or deemed to have been given.
- **Purpose limitation**
  Section 18 of the PDPA provides that an organisation may collect, use or disclose personal data about an individual only for purposes that a reasonable person would consider appropriate in the circumstances and, where applicable, if the individual concerned has been notified ("**Purpose Limitation Obligation**").
- **Data minimisation**
  The PDPA does not articulate the principle of data minimisation (i.e. the limitation of personal data collection to what is directly relevant and necessary to accomplish a specified purpose), although the Purpose Limitation Obligation and Retention Limitation Obligation (as defined below) operate to limit the collection, use, disclosure and retention of personal data by organisations to some extent.
  Nonetheless, the PDPC recommends that organisations avoid the over-collection of personal data where this is not required for their business or legal purposes. Instead, the PDPC encourages organisations to consider whether there are alternative ways of addressing their requirements.
- **Proportionality**
  While the PDPA does not explicitly refer to the principle of proportionality, a number of the Data Protection Provisions – for instance, the Purpose Limitation Obligation, the Accuracy Obligation, the Protection Obligation, and the Retention Limitation Obligation (as defined below) – make reference to a standard of reasonableness.
  More generally, Section 11(1) of the PDPA states that an organisation shall, in meeting its responsibilities under the PDPA, "*consider what a reasonable person would consider appropriate in the circumstances*".
  In this regard, the PDPC's Key Concepts Guidelines state that a "reasonable person" is judged based on an objective standard and can be said to be a person who exercises the appropriate care and judgment in the particular circumstances.
- **Retention**
  While the PDPA does not prescribe any specific data retention periods, Section 25 of the PDPA provides that an organisation must cease to retain documents containing personal data, or remove the means by which the personal data can be associated with particular individuals as soon as it is reasonable to assume that (a) the purpose for which the personal data was collected is no longer being served by retention of the personal data, and (b) retention is no longer necessary for legal or business purposes ("**Retention Limitation Obligation**").
- **Other key principles**
  - Section 23 of the PDPA requires an organisation to make a reasonable effort to ensure that personal data collected by or on behalf of the organisation is accurate and complete, if the personal data is likely to be used by the organisation to make a decision that affects the individual to whom the personal data relates, or is likely to be disclosed by the organisation to another organisation ("**Accuracy Obligation**").
  - Section 24 of the PDPA requires an organisation to make reasonable security arrangements to protect personal data in its possession or under its control, in order to prevent (i) unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks, and (ii) the loss of any storage medium or device on which personal data is stored. ("**Protection Obligation**") (see our response to section 15 below).
  - Section 26 of the PDPA provides that an organisation must not transfer any personal data to a country or territory outside Singapore, except in accordance with prescribed requirements to ensure that organisations provide a standard of protection to the transferred personal data that is comparable to the protection under the PDPA ("**Transfer Limitation Obligation**") (see our responses in section 11 below).

## 5 Individual Rights

### 5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**
  Under Section 21 of the PDPA, an individual has the right to request an organisation to allow him access to his personal data.
  Specifically, unless a relevant exception under the PDPA applies, an organisation is required to, on request by an

individual, provide him with: (a) his personal data in the possession or under the control of the organisation; and (b) information about the ways in which that personal data has been or may have been used or disclosed by the organisation within a year before the date of the individual's request ("**Access Obligation**").

There are a number of exceptions to the Access Obligation. Specifically, an organisation is not required to provide an individual with his personal data or other information, in respect of the matters specified under the Fifth Schedule to the PDPA, which include, without limitation:

- opinion data kept solely for an evaluative purpose;
- personal data which, if disclosed, would reveal confidential commercial information that could, in the opinion of a reasonable person, harm the competitive position of the organisation;
- personal data collected, used or disclosed without consent, for the purposes of an investigation if the investigation and associated proceedings and appeals have not been completed; and
- any request:
  - that would unreasonably interfere with the operations of the organisation because of the repetitious or systematic nature of the requests;
  - where the burden or expense of providing access would be unreasonable to the organisation or disproportionate to the individual's interests;
  - for information that does not exist or cannot be found;
  - for information that is trivial; or
  - that is otherwise frivolous or vexatious.

  In addition, Section 21(3) of the PDPA provides that an organisation shall not provide an individual with his personal data or other information, if doing so could be reasonably expected to:
  - threaten the safety or physical or mental health of an individual other than the individual who made the request;
  - cause immediate or grave harm to the safety or to the physical or mental health of the individual who made the request;
  - reveal personal data about another individual;
  - reveal the identity of an individual who has provided personal data about another individual and the individual providing the personal data does not consent to the disclosure of his identity; or
  - be contrary to the national interest.

With respect to third-party personal data, certain exclusion(s) do not apply to any user activity data about, or any user-provided data from, the individual who made the request despite such data containing personal data about another individual.

- **Right to rectification of errors**

  Under Section 22 of the PDPA, an individual has the right to request that an organisation correct an error or omission in his personal data.

  Specifically, an organisation is required to, on request by an individual: (a) correct an error or omission in the individual's personal data that is in the possession or under the control of the organisation; and (b) send the corrected personal data to every other organisation to which the personal data was disclosed by the organisation within a year before the date the correction request was made, unless that other organisation does not need the corrected personal data for any legal or business purpose ("**Correction Obligation**").

  However, Section 22(7) of the PDPA provides that an organisation is not required to comply with the Correction Obligation in respect of the following matters specified in the Sixth Schedule to the PDPA:
  - opinion data kept solely for an evaluative purpose;
  - any examination conducted by an education institution, examination scripts and, prior to the release of examination results, examination results;
  - the personal data of the beneficiaries of a private trust kept solely for the purpose of administering the trust;
  - personal data kept by an arbitral institution or a mediation centre solely for the purposes of arbitration or mediation proceedings administered by the arbitral institution or mediation centre;
  - a document related to a prosecution if all proceedings related to the prosecution have not been completed; and
  - derived personal data.

  In addition, Section 22(6) of the PDPA provides that an organisation is not required to correct or otherwise alter an opinion, including a professional or an expert opinion.
- **Right to deletion/right to be forgotten**

  The PDPA does not accord an individual the right to require an organisation to delete his personal data.
- **Right to object to processing**

  Under Section 16 of the PDPA, an individual may, upon giving reasonable notice to an organisation, withdraw his consent (which includes deemed consent) given to the organisation for the collection, use, or disclosure of his personal data for any purpose. Upon withdrawal of consent, the organisation must cease (and cause its data intermediaries and agents to cease) collecting, using or disclosing the personal data, as the case may be, unless the collection, use or disclosure of the personal data without consent is required or authorised under the PDPA or any other written law.
- **Right to restrict processing**

  Please see our response to "Right to object to processing" above.
- **Right to data portability**

  The Amendment Act has introduced a Data Portability Obligation, which is set out in Part VIB of the PDPA. However, it has yet to come into effect and will only do so after 1 February 2022.

  Broadly, the Data Portability Obligation provides that subject to certain exceptions and conditions, upon an organisation's receipt of a data porting request from an individual, the porting organisation must transmit the applicable data specified in the data porting request to the receiving organisation in accordance with any prescribed requirements.
- **Right to withdraw consent**

  Please see our response to "Right to object to processing" above.
- **Right to object to marketing**

  Please see our response to "Right to object to processing" above.

  In addition, an individual who does not wish to receive specified telemarketing calls and messages addressed to his Singapore telephone number may register his Singapore telephone number on one or more of the three DNC registers (namely, the No Voice Call Register; the No Text Message Register; and the No Fax Message Register) (see our response to question 9.1 below).
- **Right to complain to the relevant data protection authority(ies)**

  An individual may lodge a complaint with the PDPC in

respect of an organisation's breach of any of the Data Protection Provisions or DNC Provisions. Upon receiving such a complaint, the PDPC may: direct the individual and the organisation to resolve the complaint; refer the matter for mediation; or conduct an investigation to determine whether or not the organisation is in compliance with the PDPA.

## 6 Registration Formalities and Prior Approval

**6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?**

There is currently no requirement for organisations to register with or notify the PDPC.

**6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?**

This is not applicable in Singapore.

**6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?**

This is not applicable in Singapore.

**6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?**

This is not applicable in Singapore

**6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?**

This is not applicable in Singapore.

**6.6 What are the sanctions for failure to register/notify where required?**

This is not applicable in Singapore.

**6.7 What is the fee per registration/notification (if applicable)?**

This is not applicable in Singapore.

**6.8 How frequently must registrations/notifications be renewed (if applicable)?**

This is not applicable in Singapore.

**6.9 Is any prior approval required from the data protection regulator?**

This is not applicable in Singapore.

**6.10 Can the registration/notification be completed online?**

This is not applicable in Singapore.

**6.11 Is there a publicly available list of completed registrations/notifications?**

This is not applicable in Singapore.

**6.12 How long does a typical registration/notification process take?**

This is not applicable in Singapore.

## 7 Appointment of a Data Protection Officer

**7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.**

The appointment of a Data Protection Officer ("**DPO**") is mandatory. Section 11(3) of the PDPA obliges an organisation to "*designate one or more individuals to be responsible for ensuring that the organisation complies with [the PDPA]*".

The business contact information of at least one DPO must be made available to the public (e.g. email address or Singapore phone number) and be readily accessible from Singapore, operational during Singapore business hours and, in the case of telephone numbers, be Singapore telephone numbers. This is especially important if the DPO is not physically based in Singapore, as it would facilitate the organisation's ability to respond promptly to any complaint or query on its data protection policies and practices.

**7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?**

Generally, the PDPC may take the following enforcement actions against the organisation:

(a) give the organisation such directions as the PDPC sees fit in the circumstances to ensure compliance; and/or

(b) require the organisation to pay a financial penalty of such amount not exceeding S$1 million as the PDPC sees fit. The Amendment Act will empower the PDPC to impose higher financial penalties (i.e. up to a maximum of 10% of the organisation's annual turnover in Singapore, or S$1 million, whichever is higher). However, this provision will only come into effect after 1 February 2022.

**7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?**

The PDPA does not provide for any particular protections for

DPOs in respect of their role as DPOs. However, to the extent that the DPO is an employee of the organisation, Section 4(1)(a) of the PDPA provides that the Data Protection Provisions do not apply to an employee acting in the course of his employment.

It should be noted that the appointment of a DPO does not relieve the organisation of its obligations and liabilities under the PDPA.

**7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?**

Yes. Section 11(3) of the PDPA only provides that each organisation "*shall designate one or more individuals to be responsible for ensuring that the organisation complies with [the PDPA]*", but does not stipulate that organisations may not designate individuals already designated by other organisations. Section 11(4) of the PDPA further provides that an individual designated by an organisation may further delegate the responsibility conferred by that delegation on another individual. For the avoidance of doubt, the designated individual need not be an employee of the organisation.

**7.5 Please describe any specific qualifications for the Data Protection Officer required by law.**

There are no specific qualifications required by law of the DPO. In practice, however, it would be advisable that an organisation appoint an individual (or a group of individuals) familiar with the data protection laws of Singapore, the organisation's data protection policies and procedures, as well as its data processing activities. This is to ensure that the DPO is well equipped to: (i) ensure the organisation's continued compliance with the PDPA; (ii) deal with any queries from authorities or the public in relation to the organisation's data protection practices; and (iii) limit the impact of any data breach incident.

The PDPC has also published the DPO Competency Framework and Training Roadmap to provide clarity on the competencies and proficiency levels which a DPO needs, and to assist organisations in the hiring and training of data protection professionals.

**7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?**

The DPO is responsible for ensuring the organisation's continued compliance with the PDPA. However, it should be noted that the appointment of a DPO does not relieve the organisation of its obligations and liabilities under the PDPA.

Some of the responsibilities of a DPO may include, but are not limited to:

- ensuring compliance with the PDPA when developing and implementing policies and processes for handling personal data;
- fostering a data protection culture among employees and communicating personal data protection policies to stakeholders;
- managing personal data protection-related queries and complaints;
- alerting management to any risks that might arise with regard to personal data; and
- liaising with the PDPC on data protection matters, if necessary.

**7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?**

No, there is no requirement for the DPO to be registered with or notified to the PDPC. However, DPOs are encouraged to subscribe to the PDPC's *DPO Connect* newsletter in order to keep abreast of developments in the PDPA.

**7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?**

No. However, the business contact information of at least one DPO must be made available to the public.

## 8 Appointment of Processors

**8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?**

There is no strict requirement for an agreement between the organisation and data intermediary under the PDPA. However, it should be noted that appointing a data intermediary to process personal data does not relieve the organisation of its obligations and liabilities under the PDPA, as the organisation is deemed to "*have the same obligation under [the PDPA] in respect of personal data processed on its behalf and for its purposes by a data intermediary as if the personal data were processed by the organisation itself*".

The Key Concepts Guidelines state that it is important that an organisation is clear as to its rights and obligations when dealing with another organisation and, where appropriate, include provisions in their written contracts to clearly set out each organisation's responsibilities and liabilities in relation to the personal data in question, including whether one organisation is to process personal data on behalf of and for the purposes of the other organisation. If there is no contract evidenced or made in writing with the data organisation, the data intermediary will need to comply with all the Data Protection Provisions in respect of the personal data that is processed on behalf of the data organisation.

Furthermore, where an organisation engages a data intermediary, the organisation is responsible for complying with the Transfer Limitation Obligation in respect of any overseas transfer of personal data (i.e. by the organisation to the overseas data intermediary, or by the data intermediary itself as part of the processing) (see section 11 below). To comply with the Transfer Limitation Obligation, the organisation may need to undertake appropriate due diligence and obtain assurances from the data intermediary, and/or ensure that the recipient is bound by legally enforceable obligations, which may include a contract fulfilling the requirements under the PDP Regulations.

**8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?**

As the organisation remains responsible for complying with the PDPA notwithstanding that a data intermediary is processing personal data on its behalf, it may be prudent for the organisation to impose specific obligations on its data intermediary through a written agreement, including restricting what the data intermediary may do with the disclosed personal data, having sufficient security measures to protect the disclosed personal data, and providing for audits, inspections, or other types of spot checks to satisfy itself that the data intermediary is complying with the PDPA.

If it is contemplated that there will be overseas transfers of personal data, the agreement may provide assurances to ensure that the personal data is protected to a standard comparable with the PDPA, along with other policies and practices (e.g. assurances of compliance with relevant industry standards/certification). See "Transfer Limitation Obligation" at section 11 below.

## 9 Marketing

**9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).**

The PDPA and the SCA concurrently govern the sending of such direct marketing messages in Singapore.

Generally, where the personal data of an individual is collected, used and disclosed for marketing purposes, the consent of the individual concerned must be obtained and such consent must not have been obtained as a condition for the providing of a product or service where it would not be reasonably required to provide that product or service. This applies regardless of how the marketing communications are sent.

In this regard, the PDPC has noted in its Key Concepts Guidelines that a failure to opt out will not be regarded as consent in all situations, and has recommended that organisations obtain consent from an individual through a positive action of the individual. It would therefore be advisable to obtain prior opt-in consent instead.

In relation to the sending of marketing communications (i.e. "specified messages" as defined under Section 37 of the PDPA) by telephone call or text messaging (or fax) to a Singapore telephone number, the DNC Provisions of the PDPA require an organisation to:

(a) obtain valid confirmation that the telephone number is not listed with the relevant DNC Registry before sending the message or calling, unless clear and unambiguous consent to the sending of the specified message to that number is obtained in evidential form;
(b) include information identifying the sender for messages and details on how the sender can be readily contacted and such details and contact information should be reasonably likely to be valid for at least 30 days after the sending of the message;
(c) for voice calls, not conceal or withhold the calling line identity from the recipient; and
(d) not to send, cause to be sent, or authorise the sending of an applicable message to any telephone number generated or obtained through the use of: (a) a dictionary attack; or (b) address-harvesting software.

In relation to the sending of unsolicited marketing communications in bulk by email, instant messaging or other electronic messaging means, Section 11 read with the Second Schedule of the SCA stipulates that such messages must contain, *inter alia*, the following:

(a) information on the sender;
(b) a clear and conspicuous statement in English setting out the procedure to unsubscribe;
(c) a title in its subject field that is not false or misleading as to the content of the message';
(d) a label "<ADV>" with a space before the title of the subject field or, in the absence of a subject field, the first word of the message;
(e) header information that is not false or misleading; and
(f) an accurate and functional email address or telephone number by which the sender is readily contactable.

The unsubscribe facility must be legitimately obtained, valid and capable of receiving the unsubscribe request and a reasonable number of similar unsubscribe requests sent by other recipients at all times within at least 30 days after the unsolicited message is sent. No further unsolicited marketing communications can be sent after 10 business days following the date of the unsubscribe request.

Furthermore, Section 9 of the SCA prohibits unsolicited commercial electronic messages in bulk from being sent to electronic addresses generated or obtained through the use of a dictionary attack or address-harvesting software.

**9.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?**

Generally, the direct marketing restrictions in the PDPA only apply in the business-to-consumer ("**B2C**") context where an organisation sends direct marketing communications to individual consumers. Insofar as an organisation sends direct marketing messages to another organisation through the use of business contact information, i.e. business-to-business ("**B2B**") messages, the Data Protection Provisions in the PDPA would likely not be applicable in those instances.

In specific relation to the sending of specified messages (as defined in Section 37 of the PDPA) by telephone call, text messaging, or fax to a Singapore telephone number, paragraph 1(g) of the Eighth Schedule of the PDPA provides that a "specified message" shall exclude "*any message sent to an organisation other than an individual acting in a personal or domestic capacity, for any purpose of the receiving organisation*". In other words, a B2B marketing message would not be considered a "specified message", and the organisation that sent such a B2B message would not need to comply with requirements under the DNC Provisions.

Notwithstanding, B2B marketing is currently covered under the SCA, and the restrictions on such electronic messages (see question 9.1 above) would similarly apply.

**9.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).**

Please see our response to question 9.1 above.

**9.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?**

Yes, if the recipient of the marketing messages is present in Singapore when the marketing message is accessed. With respect to the collection, use and disclosure of personal data for marketing purposes, the Data Protection Provisions of the PDPA apply to all organisations, whether or not formed or recognised under the laws of Singapore, or resident or having an office or a place of business in Singapore.

Specifically, the DNC Provisions under the PDPA apply when the sender of the specified message is present in Singapore when the specified message is sent, or the recipient of the specified message is present in Singapore when the specified message is accessed.

The SCA applies as long as the electronic message has a Singapore link, which includes, *inter alia*, the following situations:

- the message originates in Singapore or the sender of the message is: (i) an individual who is physically present in Singapore when the message it sent; or (ii) an entity which is formed or recognised under the law of Singapore, or which has an office or a place of business in Singapore;
- the computer, mobile telephone, server or device that is used to access the message is located in Singapore; or
- the recipient of the message is, when the message is accessed: (i) an individual who is physically present in Singapore; or (ii) an entity that carries on business or activities in Singapore.

**9.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?**

The PDPA is a complaints-based regime and the PDPC has been active in the enforcement of breaches thereof.

Since the commencement of the PDPA in 2014, the PDPC has charged several individuals for offences relating to breaches of the DNC Registry.

**9.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?**

Purchasing marketing lists from third parties is only lawful if the individuals whose personal data is contained within the lists are notified of, and consent to, the sale of their personal data before such data is collected, used, and/or disclosed.

The purchase of marketing lists constitutes collecting personal data under the PDPA. The PDPC has taken enforcement action against organisations which have purchased marketing lists without obtaining valid consent. For example, in the decision of *Re Sharon Assya Qadriyah Tang* [2018] SGPDPC 1, the PDPC imposed a financial penalty of S$6,000 on an individual for buying and selling marketing lists containing personal data.

Similarly, the PDPC took action in the case of *Re Amicus Solutions Pte Ltd & Anor* [2019] SGPDPC 33, which involved the unauthorised sale and disclosure of personal data by a data broker for telemarketing purposes. In that case, the PDPC stated that organisations that sell datasets should ensure that they obtain and maintain clear records of consent so that proper assurances can be given to buyers. Correspondingly, buyers should undertake proper due diligence, such as seeking written confirmation that the personal data sold was actually obtained via legal sources or means, or inquire further as to whether the individuals had provided their consent and were notified of the disclosure, and if so, obtain a sample of such consent and notification. On the facts, the PDPC imposed a fine of S$48,000 on the data seller (including the S$2,900 for the profit that the seller made from the sale of the datasets), and a fine of S$10,000 on the buyer.

**9.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?**

In relation to a breach of the Data Protection Provisions that apply to the sending of marketing communications, the organisation may find itself liable to pay a financial penalty of up to S$1 million (see question 7.2 above).

In relation to the DNC Provisions, the Amendment Act brings contraventions of the DNC Provisions (which used to be enforced as criminal offences), under the same administrative regime as the Data Protection Provisions. Accordingly, if the organisation is found to have intentionally or negligently contravened any provision, the PDPC may require the organisation to pay a financial penalty not exceeding:

(a) S$200,000, in case of an individual; or
(b) S$1 million, in any other case.

For contravention of the provisions prohibiting the use of dictionary attacks and address-harvesting software under the DNC Provisions, the maximum financial penalty has been increased to 5% of the annual turnover of the organisation in Singapore, where the annual turnover in Singapore exceeds $20 million. However, this provision will only come into effect after 1 February 2022.

These offences are in addition to the rights of private action that individuals may have against the organisation under the PDPA and the SCA.

## 10 Cookies

**10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).**

There are presently no legislative restrictions on the use of cookies or similar technologies *per se*, although the PDPA will apply to cookies that collect or use personal data.

According to the Advisory Guidelines on the PDPA for Selected Topics, for Internet activities that the user has clearly requested (e.g. transmitting personal data for effecting online communications and storing information that the user enters in a web form to facilitate an online purchase), there may not be a need to seek consent for the use of cookies to collect, use, and disclose personal data where the individual is aware of the purposes for such collection, use or disclosure and voluntarily provided his personal data for such purposes. For activities that cannot take place without cookies that collect, use or disclose personal data, consent may be deemed if the individual voluntarily provides the personal data for that purpose of the activity, and it is reasonable that he would do so.

Consent may also be reflected in the way a user configures his interaction with the Internet. If the individual configures his browser to accept certain cookies but rejects others, he may be found to have consented to the collection, use and disclosure of his personal data by the cookies that he has chosen to accept.

**10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?**

This is not applicable in Singapore.

**10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?**

To date, the PDPC has not issued any enforcement decisions specifically in relation to cookies.

**10.4 What are the maximum penalties for breaches of applicable cookie restrictions?**

This is not applicable in Singapore.

## 11 Restrictions on International Data Transfers

**11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.**

The Transfer Limitation Obligation under the PDPA requires organisations transferring personal data abroad to do so only in accordance with the requirements prescribed under the PDPA to ensure that the recipients provide a standard of protection to personal data so transferred that is comparable to the protection under the PDPA.

In particular, under the PDP Regulations, the transferring organisation must, before transferring the personal data outside of Singapore:

- take appropriate steps to ensure that the transferring organisation continues to comply with the Data Protection Provisions in respect of the personal data being transferred so long as such personal data remains in its possession or under its control; and
- take appropriate steps to ascertain whether, and to ensure that, the recipient is bound by legally enforceable obligations to provide the personal data transferred with a standard of protection comparable to that provided for by the PDPA.

For completeness, the PDP Regulations provide for certain prescribed situations whereby either or both of the above requirements are taken to be satisfied, e.g., where the personal data is publicly available in Singapore or where the personal data is data in transit.

"Legally enforceable obligations" is defined in the PDP Regulations to include obligations imposed on the recipient under:

(a) any law;
(b) any contract that requires the recipient to provide to the transferred personal data a standard of protection that is at least comparable to the protection under the PDPA, and which specifies the countries and territories to which the personal data may be transferred under the contract;
(c) any binding corporate rules (in cases where a recipient is an organisation related to the transferring organisation) that require every recipient to provide to the transferred personal data a standard of protection that is at least comparable to the protection under the PDPA, and which specifies (i) the recipients of the transferred personal data to which the binding corporate rules apply, (ii) the countries and territories to which the personal data may be transferred under the binding corporate rules, and (iii) the rights and obligations provided by the binding corporate rules; or
(d) any other legally binding instrument.

The PDP Regulations also recognise the certification systems under the Asia-Pacific Economic Cooperation ("**APEC**") Cross-Border Privacy Rules ("**CBPR**") System and Privacy Recognition for Processors ("**PRP**") System as one of the modes for the transfers of data overseas. If the recipient holds a specified certification (i.e. certification under the APEC CBPR/PRP) that is granted or recognised under the law of that country or territory to which the personal data is transferred, the recipient is taken to be bound by legally enforceable obligations to provide a standard of protection for the transferred personal data that is at least comparable to the protection under the PDPA.

The PDP Regulations define a recipient as being related to the transferring organisation if:

(a) the recipient, directly or indirectly, controls the transferring organisation;
(b) the recipient is, directly or indirectly, controlled by the transferring organisation; or
(c) the recipient and the transferring organisation are, directly or indirectly, under the control of a common person.

**11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).**

Companies generally rely on robust data transfer agreements and binding corporate rules, as well as active enforcement of the terms of these documents, to ensure their compliance with applicable transfer restrictions.

See also questions 8.1 and 8.2 above with respect to overseas transfers of personal data for organisations engaging data intermediaries.

**11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.**

No, there is no requirement for registration/notification or prior approval from the PDPC for transfers of personal data abroad.

**11.4 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?**

The PDPC has not issued any guidance on this topic.

**11.5 What guidance (if any) has/have the data protection authority(ies) issued in relation to the European Commission's revised Standard Contractual Clauses?**

The PDPC has not issued any guidance on this topic. However, the PDPC has published on its website some FAQs on the applicability of the EU GDPR.

## 12 Whistle-blower Hotlines

**12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?**

The PDPA does not specifically regulate corporate whistle-blowing hotlines.

To the extent that whistle-blowing falls under the definition of "investigation" as found in the PDPA, the PDPA provides that personal data can be collected without obtaining consent if it is necessary for any investigation or proceedings. Similarly, the use and disclosure of personal data can be done without obtaining consent if it is necessary for any investigation or proceedings.

In this regard, the PDPA defines "investigation" to refer to an investigation relating to:

(a) a breach of an agreement;
(b) a contravention of any written law, or any rule of professional conduct or other requirement imposed by any regulatory authority in exercise of its powers under any written law; or
(c) a circumstance or conduct that may result in a remedy or relief being available under any law.

The PDPA also provides for a broad definition of "proceedings" to mean any civil, criminal or administrative proceedings by or before a court, tribunal or regulatory authority that is related to the allegation of:

(a) a breach of an agreement;
(b) a contravention of any written law or any rule of professional conduct or other requirement imposed by any regulatory authority in exercise of its powers under any written law; or
(c) a wrong or a breach of a duty for which a remedy is claimed under any law.

**12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?**

Anonymous reporting is not regulated under the PDPA.

## 13 CCTV

**13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?**

The PDPA does not require the use of CCTV to be separately registered/notified or approved beforehand by the PDPC. However, as video and audio recordings of individuals may constitute personal data, the use of CCTV may constitute the collection of personal data and hence an organisation must comply with the PDPA when using CCTV.

Notices or other forms of notification should generally be placed at locations that would enable individuals to have sufficient awareness that CCTV has been deployed for a particular purpose. Generally, organisations should indicate that CCTV is operating in the premises, and state the purpose of the CCTV (e.g. the CCTV is installed for security purposes) if such purpose may not be obvious to the individual. Further, where the CCTV deployed records both video and audio, organisations should indicate that both video and audio recordings are taking place.

**13.2 Are there limits on the purposes for which CCTV data may be used?**

Insofar as CCTV data contains personal data, the PDPA limits the purposes for which the CCTV data may be used.

## 14 Employee Monitoring

**14.1 What types of employee monitoring are permitted (if any), and in what circumstances?**

Employee monitoring is not specifically regulated in Singapore. To the extent that the employee monitoring results in the collection, use or disclosure of personal data under the PDPA, such monitoring will fall under the regulation of the Data Protection Provisions.

**14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.**

Before collecting, using or disclosing the personal data (which would include CCTV images/footage of such employees and the other data collected by the employer pursuant to their employee monitoring activities, to the extent that the employees can be identified from such data alone or with other information to which the organisation is likely to have access) of their employees, employers are generally required to provide suitable notices and obtain consent.

An exception to this requirement under the PDPA is where personal data is collected by the employer and the collection for the purpose of or in relation to the organisation: (a) entering into an employment relationship with the individual or appointing the individual to any office; or (b) managing or terminating the employment relationship with or appointment of the individual. Nonetheless, if the organisation wishes to rely on this exception, the organisation would need to inform the individual of the purpose, and on request by the individual, the contact information of a person who is able to answer the individual's questions on such processing.

Due to the inherent uncertainty of the ambit of this exception, it is common for employers to include related clauses in their personal data protection policies, employment handbook or employment agreements to obtain express consent from their employees prior to the commencement of employee monitoring or using CCTV surveillance. It is also not unusual for organisations to provide prominent notices at the entrances of their premises to alert visitors that their premises are monitored by CCTV. Such notices should state the purpose of the CCTV.

**14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?**

As the relationship between employers and trade unions is very much subject to the terms of the collective agreement, the necessity of notifying or consulting the trade union in respect of CCTV and employee monitoring is dependent on the terms of the collective agreement. There are generally no legal requirements under Singapore law requiring works councils/trade unions/employee representatives to be notified or consulted.

## 15 Data Security and Data Breach

**15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?**

Yes, both organisations and data intermediaries are subject to the Protection Obligation in relation to the personal data in their possession or control. For the Protection Obligation, please see our response to question 4.1 above.

While the PDPC has recognised that there is no one-size-fits-all solution, it has, in its Key Concepts Guidelines, noted that an organisation should:

- design and organise its security arrangements to fit the nature of the personal data held by the organisation and the possible harm that might result from a security breach;

- identify reliable and well-trained personnel responsible for ensuring information security;
- implement robust policies and procedures for ensuring appropriate levels of security for personal data of varying levels of sensitivity; and
- be prepared and able to respond to information security breaches promptly and effectively.

**15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

There is a mandatory data breach notification regime under Part VIA of the PDPA, which broadly requires organisations to notify the PDPC and/or affected individuals of a "notifiable data breach" within specified timeframes and in accordance with the prescribed form, unless exceptions apply.

**Duty to Assess**

Section 26C of the PDPA requires organisations to conduct, in a reasonable and expeditious manner, an assessment of whether the data breach is a notifiable data breach, if it has reason to believe that a data breach has occurred affecting personal data in its possession or under its control.

Where a data intermediary has reason to believe that a data breach has occurred in relation to personal data that the data intermediary is processing on behalf of and for the purposes of another organisation, the data intermediary must, without undue delay, notify that other organisation of the occurrence of the data breach.

**Requirement to Notify**

Under section 26D of the PDPA, where an organisation assesses that a data breach is a notifiable data breach, i.e.: where the data breach:

- results in, or is likely to result in significant harm to or impact on the individuals to whom the data relates (i.e. if the breach relates to prescribed types of data or circumstances); or
- is or is likely to be, of a significant scale (i.e. the data breach involves personal data of 500 or more individuals),

the organisation must notify the PDPC as soon as is practicable, but in any case no later than three calendar days after it makes the assessment.

The notification should be in the form and manner as prescribed in the Personal Data Protection (Notification of Data Breaches) Regulations 2021 and contain information to the best of the knowledge and belief of the organisation at the time.

**Details of Notification**

Specifically, the notification to the PDPC should include information such as:

- the date and circumstances in which the organisation first became aware that the data breach had occurred;
- an account of steps taken afterwards, including the organisation's assessment of whether the breach is notifiable;
- how the data breach occurred;
- the number of individuals affected by the data breach;
- the personal data or classes of personal data affected;
- the potential harm to the affected individuals as a result;
- any action by the organisation to: (i) eliminate or mitigate any potential harm to any affected individual; and (ii) address or remedy any failure or shortcoming that resulted in the breach;
- the organisation's plan to inform all or any affected individuals or the public or grounds for not informing the affected individuals (if applicable);
- the business contact information of at least one authorised representative; and
- the reasons for late notification and/or the grounds for not notifying affected individuals (if the organisation is otherwise required to notify), where applicable.

Notification to the PDPC is to be submitted at https://eservice.pdpc.gov.sg/case/db. For urgent notification of major cases, organisations may also contact the PDPC at +65 6377 3131 during working hours.

The PDPC's Guide on Managing and Notifying Data Breaches (updated 15 March 2021) provides further guidance to help organisations to identify, prepare for, and manage data breaches.

In addition to the Data Breach Notification Obligation under the PDPA, there may also be sector-specific requirements relating to the notification of data breaches which the organisation is subject to.

**15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

Under section 26D of the PDPA, organisations must, on or after notifying the PDPC, notify the individuals affected by a notifiable data breach, if the data breach results in, or is likely to result in, significant harm to an affected individual, unless either one of the stated exceptions apply, namely:

- where the organisations have taken remedial actions that renders it unlikely that the notifiable data breach will result in significant harm to the affected individual;
- where the personal data that was compromised by the data breach is subject to technological protection (e.g. encryption) that renders it unlikely that the notifiable data breach will result in significant harm to the affected individual; or
- where organisations are prohibited from notifying the affected individuals (i.e. if a prescribed law enforcement agency so instructs them). In addition, the PDPC may, on written application, waive the requirement in exceptional circumstances where notification to affected individuals may not be desirable.

The notification to affected individuals should contain the following:

- the circumstances in which the organisation first became aware that the data breach had occurred;
- the personal data or classes of personal data affected;
- the potential harm to the affected individuals as a result;
- any action by the organisation to: (i) eliminate or mitigate any potential harm to any affected individual; and (ii) address or remedy any failure or shortcoming that resulted in the breach;
- the steps that the affected individual may take to eliminate or mitigate any potential harm as a result, including preventing the misuse of the data; and
- contact details of at least one authorised representative whom the affected individual can contact for further information or assistance.

The notification should be in the form and manner as prescribed in the Personal Data Protection (Notification of Data Breaches) Regulations 2021 and contain information to the best of the knowledge and belief of the organisation at the time.

### 15.4 What are the maximum penalties for data security breaches?

The PDPC has discretion to issue such remedial directions as it sees fit, including a direction to require payment of a financial penalty of up to S$1 million. As stated above, the Amendment Act will empower the PDPC to impose higher financial penalties (i.e. up to a maximum of 10% of the organisation's annual turnover in Singapore, or S$1 million, whichever is higher). However, this provision will only come into effect after 1 February 2022.

On 15 January 2019, the PDPC imposed its highest financial penalties to date, of S$250,000 and S$750,000 respectively, on SingHealth Services Pte Ltd ("**SingHealth**") and Integrated Health Information Systems Pte Ltd, for breaching their data protection obligations under the PDPA. This unprecedented data breach, which arose from a cyberattack on SingHealth's patient database system, caused the personal data of some 1.5 million patients to be compromised.

## 16 Enforcement and Sanctions

### 16.1 Describe the enforcement powers of the data protection authority(ies).

**Powers of Investigation**

The Ninth Schedule of the PDPA sets out extensive powers of investigation of the PDPC and its inspectors, which includes the power to: (i) require documents or information; (ii) require provision of information (e.g. to require attendance of individuals); and (iii) enter premises with or without a court-issued search warrant.

Section 51 of the PDPA sets out certain offences relating to, amongst others, obstructing or hindering the PDPC in the performance of any function or duty, or the exercise of any power, under the PDPA. It is also an offence for an organisation or a person, without reasonable excuse, to neglect or refuse to either provide any information or produce any document which the organisation or person is required to provide or produce to the PDPC or an inspector, or attend before the PDPC or inspector as required.

**Power to Review**

On application of a complainant, the PDPC may review: (i) refusals to provide access to personal data or to correct personal data as requested by the complainant under the PDPA or a failure to provide such access or correction within a reasonable time; (ii) a refusal by a porting organisation to transmit any applicable data, or a failure to transmit within a reasonable time; or (iii) a fee required from the complainant by an organisation in relation to a request by the complainant under the PDPA.

Upon reviewing, the PDPC may: (i) confirm the refusal to provide access to, correct the personal data (as the case may be) and direct the organisation to provide access to or correct the personal data (as the case may be) within a specified timeframe; or (ii) confirm, reduce or disallow a fee, or direct the organisation to make a refund to the complainant.

**Power to Issue Directions**

The PDPC may issue such directions as it thinks fit in the circumstances to ensure compliance by an organisation with the PDPA. These include directions to: (i) stop collecting, using or disclosing personal data in contravention of the PDPA; (ii) destroy personal data collected in contravention of the PDPA; (iii) comply with any direction of the PDPC; and (iv) pay a financial penalty. (Please see question 7.2 above on the quantum of the financial penalty.)

**Voluntary Undertakings**

Section 48L of the PDPA empowers the PDPC to accept statutory undertakings. Under this new section, where the PDPC has reasonable grounds to believe that an organisation has not complied, is not complying or is likely not to comply with any of the data protection provisions, the organisation may give, and the PDPC may accept a written voluntary undertaking.

**Alternative Dispute Resolution**

Section 48G of the PDPA empowers the PDPC to establish or approve one or more dispute resolution schemes for the resolution of complaints by mediation, and to make regulations relating to the operation of such schemes. The PDPC may, with or without the parties' consent, refer the matter to mediation under a dispute resolution scheme, if it is of the view that the matter may more appropriately be resolved in this manner.

The PDPC has issued a Guide on Active Enforcement which articulates the PDPC's approach in deploying its enforcement powers to act effectively and efficiently on data breach incidents. The guide also reiterates the PDPC's general approach to maximise the use of facilitation and mediation in seeking a resolution between the complainant and the organisation concerned.

### 16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The PDPC is empowered to direct an organisation to stop collecting, using, or disclosing personal data in contravention of the PDPA.

The PDPC does not require a court order to issue directions. Nonetheless, the PDPC may apply for the direction to be registered in a District Court for the purposes of enforcement by the court.

### 16.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

The PDPC takes a pragmatic approach in administering and enforcing the PDPA and aims to balance the need to protect individuals' personal data and the needs of organisations to use the data for legitimate purposes.

Since 2016, the PDPC has published over 100 enforcement decisions, with a significant majority of these cases relating to breaches of the Protection Obligation. In respect of these cases, the PDPC has either issued the organisation a warning, or imposed directions requiring the infringing organisation to take remedial action and to pay financial penalties.

Examples of recent cases include the following:

- A financial penalty of S$120,000 was imposed on Secur Solutions Group for a breach of the Protection Obligation. The PDPC found that Secur Solutions Group failed to put in place reasonable security arrangements to protect a database containing the personal data of blood donors from being publicly accessible online.

- A financial penalty of S$7,500 was imposed on Majestic Debt Recovery Pte Ltd for breaches of the Consent and Accountability Obligations. The PDPC found that Majestic Debt Recovery did not have any data protection policies or practices, and had not appointed a DPO. The PDPC also found that the organisation had failed to obtain consent to record the debt collection process and upload the video recordings onto its Facebook page.
- A financial penalty of S$29,000 was imposed on Tripartite Alliance Limited for a breach of the Protection Obligation. The PDPC found that the organisation had failed to put in place reasonable security arrangements to prevent the unauthorised access of approximately 20,000 individuals' and companies' data stored in its customer relationship system database.

### 16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

We have not sighted a published decision whereby the PDPC has exercised its powers against companies established in other jurisdictions with no presence in or nexus to Singapore. That said, the PDPC investigated a company established overseas which collected the personal data of Singapore residents through a registered branch office (see, e.g. *Re Cigna Europe Insurance Company S.A.-N.V.* [2019] SGPDPC 18).

Nonetheless, the PDPC is empowered to enter into a cooperation agreement with a foreign data protection authority for data protection matters such as cross-border cooperation. Specifically, under Section 10 of the PDPA, cooperation agreements may be entered into for the purposes of:

- facilitating cooperation between the PDPC and another foreign data protection authority in the performance of their respective functions insofar as those functions relate to data protection; and
- avoiding duplication of activities by the PDPC and another foreign data protection authority, where those activities involve the enforcement of data protection laws.

The PDPC may also furnish information to a foreign data protection body pursuant to a cooperation agreement, subject to the fulfilment of certain prescribed conditions.

The PDPC is also a participant of the APEC Cross-Border Privacy Enforcement Arrangement, which creates a framework for the voluntary sharing of information and provision of assistance for privacy enforcement-related activities.

## 17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

### 17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Generally, organisations must ensure that any transfers of personal data outside of Singapore comply with the requirements under the PDPA (see our responses in section 11 above). It is not uncommon for Singapore businesses to include, in their privacy policy, a general notice that any personal data they collect may be disclosed to foreign law enforcement agencies or in relation to investigations and legal proceedings.

### 17.2 What guidance has/have the data protection authority(ies) issued?

The PDPC has not issued any specific guidance yet in relation to foreign e-discovery requests or requests for disclosure from foreign law enforcement agencies.

## 18 Trends and Developments

### 18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

Breaches of the Protection Obligation under the PDPA continue to constitute the majority of enforcement decisions issued by the PDPC, with the majority of cases over the past 12 months involving the Protection Obligation.

### 18.2 What "hot topics" are currently a focus for the data protection regulator?

**Data Protection Trustmark Certification Scheme**

On 9 January 2019, the IMDA launched the Data Protection Trustmark ("**DPTM**") certification scheme for the CBPR and PRP systems, which was developed by the PDPC. The certification establishes a robust data governance standard to help businesses increase their competitive advantage and build trust with their customers. The certification requirements are based on parameters including relevance to the PDPA, international standards (e.g. APEC CBPR/PRP requirements) and industry best practices.

**Model Artificial Intelligence Governance Framework**

On 23 January 2019, the PDPC issued a Model Artificial Intelligence Governance Framework ("**Model AI Framework**") for public consultation and pilot adoption. This accountability-based framework helps chart the language and frame the discussions around harnessing AI in a responsible way.

On 21 January 2020, the PDPC released the second edition of the Model AI Framework, accompanied by the Implementation and Self-Assessment Guide for Organisations ("**ISAGO**") and the Compendium of Use Cases. On 16 October 2020, the Compendium of AI Use Cases Volume 2 was issued.

The former aims to help organisations assess the alignment of their AI governance practices with the Model AI Framework, while the latter provides case studies as to how local and international organisations across different sectors and sizes have implemented or aligned their AI governance practices with all sections of the Model AI Framework.

**Job Redesign in the Age of AI**

On 4 December 2020, the IMDA and the PDPC released the Guide to Job Redesign in the Age of AI, which adopts an industry agnostic and human-centric approach to show how existing job roles can be redesigned to harness the potential of AI, so that the value of employees' work can be increased.

**ASEAN Data Management Framework and Model Contractual Clauses**

On 22 January 2021, the ASEAN Digital Ministers' Meeting ("**ADGMIN**") approved the ASEAN Data Management

Framework ("**DMF**") and Model Contractual Clauses for Cross Border Data Flows ("**MCCs**"). The initiatives were developed by the Working Group on Digital Data Governance chaired by Singapore. The DMF provides a guide for businesses and SMEs to put in place a data management system, which includes data governance structures and safeguards. While the MCCs are template contractual terms and conditions that may be included in the binding legal agreements between businesses transferring personal data to each other across borders.

**Recent Amendments to the PDPA**

As stated above, the PDPA has recently undergone its first comprehensive review since its enactment, and the amendments are set out in the Amendment Act, which was passed in Parliament on 2 November 2020, and has mostly come into effect on 1 February 2021. Accompanying regulations have been issued, and the PDPC has updated its advisory guidelines to reflect the amendments. Some of the key changes in the law (e.g. the introduction of the Data Breach Notification Obligation) have been set out above, and others include:

- the criminalisation of egregious mishandling, by individuals, of personal data in the possession of or under the control of an organisation or a public agency (see Part IXB of the PDPA);
- the expansion of the concept of deemed consent to include two more situations: (i) deemed consent by contractual necessity; and (ii) deemed consent by notification (see section 15 of the PDPA); and
- the introduction of two new exceptions to the Consent Obligation, specifically: (i) the Legitimate Interests Exception (Part 3 of the First Schedule); and (ii) the Business Improvement Purposes Exception (Part 5 of the First Schedule, and Division 2, Part 2 of the Second Schedule).

**Lim Chong Kin** heads Drew & Napier's Technology, Media and Telecommunications Practice Group, and is co-head of the firm's Data Protection, Privacy & Cyber-security Practice.

Under Chong Kin's leadership, these Practices are consistently ranked as the leading practices in Singapore. His clients include the telecoms and media regulators, global carriers, technology market leaders, global broadcasters and content providers.

Chong Kin has been an external legal and regulatory advisor for the Personal Data Protection Commission of Singapore since 2013, and he played a key role in the liberalisation of Singapore's telecoms, media and postal sectors, where he drafted the competition frameworks.

Chong Kin is highly regarded by his peers, clients and rivals alike for his expertise, and is consistently recommended as a leading lawyer by major international legal publications such as *Chambers Asia-Pacific*, *The Legal 500 Asia Pacific*, *Who's Who Legal*, *The Guide to the World's Leading Competition & Antitrust Lawyers/Economists*, *Global Competition Review*, *Practical Law Company – Which Lawyer?*, *Asialaw Profiles* and *Best Lawyers*.

**Drew & Napier LLC**
10 Collyer Quay
10th Floor, Ocean Financial Centre
Singapore 049315

Tel: +65 6531 4110
Email: chongkin.lim@drewnapier.com
URL: www.drewnapier.com

Drew & Napier LLC has provided exceptional legal advice and representation to discerning clients since 1889 and is one of the leading and largest law firms in Singapore.

The firm has been at the forefront of the development of data protection laws in Singapore, given its extensive experience in assisting Singapore's data protection authority, the Personal Data Protection Commission ("**PDPC**"), in setting up the implementing data protection laws in Singapore. The firm continues to represent the PDPC (and its parent statutory board, the Info-communications Media Development Authority ("**IMDA**")) in advisory, enforcement and policy work.

As a testament to its expertise, the firm is listed as one of the world's top 100 data law firms in *Global Data Review*'s inaugural GDR 100 2021, and is noted for providing "*a seamless and personalised service that gives you surety that the lawyers in charge are considering your matters after putting down the phone*".

**www.drewnapier.com**

DREW & NAPIER

# Slovenia

Nataša Pirc Musar

Rosana Lemut Strle

Law Firm Pirc Musar & Lemut Strle Ltd

## 1 Relevant Legislation and Competent Authorities

### 1.1 What is the principal data protection legislation?

The Data Protection Act-1 (*Zakon o varstvu osebnih podatkov*, or ZVOP-1), Official Gazette 94/07 and 177/20, is still valid, but only in part, while the General Data Protection Regulation (GDPR) is the main act. Slovenia is the only EU Member State that did not enact a national post-GDPR data protection act (as at June 2021).

### 1.2 Is there any other general legislation that impacts data protection?

The most important statute regarding data protection is GDPR and, in some parts, ZVOP-1 (biometrics, CCTV, direct marketing not connected to emails, SMS and MMS communication, some specific measures regarding data security and data of deceased persons). Slovenia (on grounds of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016) enacted the Act on the Protection of Personal Data in the Area of Treatment of Criminal Offences on 20 November 2020, Official Gazette 177/20. The act entered into force on 31 December 2020.

### 1.3 Is there any sector-specific legislation that impacts data protection?

Various special laws as *lex specialis* contain additional, sector-specific rules on data protection; for instance, in the fields of telecommunication and on patients and employees' rights. The national Electronic Communications Act (ECA) contains rules about direct e-marketing (implementing EU ePrivacy Directive rules), and the national Patients' Rights Act defines patients' and their relatives' and other persons' rights for accessing medical data. Many sectoral laws define the content of data filing systems for the private and public sectors, including data storage time limitations.

### 1.4 What authority(ies) are responsible for data protection?

The Information Commissioner of the Republic of Slovenia (IC) (https://www.ip-rs.si/) is responsible for data protection, and for direct e-marketing it is AKOS – the Communications Networks and Services Agency of the Republic of Slovenia (https://www.akos-rs.si/en).

## 2 Definitions

### 2.1 Please provide the key definitions used in the relevant legislation:

- "**Personal Data**"
  Any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- "**Processing**"
  Any operation or set of operations that is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- "**Controller**"
  The natural or legal person, public authority, agency or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
- "**Processor**"
  A natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller.
- "**Data Subject**"
  An identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- "**Sensitive Personal Data**"
  Special categories of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
- "**Data Breach**"
  A breach of security leading to the accidental or unlawful

destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

- *Other key definitions – please specify (e.g., "Pseudonymous Data", "Direct Personal Data", "Indirect Personal Data")*
  Other key definitions are the same as those in the GDPR.

## 3 Territorial Scope

### 3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

ZVOP-1 (Article 5), still valid in this section, applies to the processing of personal data if the data controller is established or registered in Slovenia or if the branch of the personal data controller is registered in Slovenia. ZVOP-1 also applies if the data controller is not established or is not registered in a Member State of the EU or is not part of the European Economic Area and uses automated or other equipment located in Slovenia for the processing of personal data if this equipment is used only for the transfer of personal data through the territory of Slovenia. The controller of personal data must determine the natural or legal person established or registered in Slovenia who represents it regarding the processing of personal data.

Regarding exterritoriality, GDPR is also applicable to businesses for the processing of personal data in the context of the activities of an establishment of a controller or a processor in the EU, regardless of whether the processing takes place in any Member State or not.

GDPR applies to the processing of personal data of data subjects who are in the EU by a controller or processor not established in the EU, where the processing activities are related to the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the EU, or the monitoring of their behaviour as far as their behaviour takes place within the EU.

GDPR also applies to the processing of personal data by a controller not established in the EU, but in a place where Member State law applies by virtue of public international law.

## 4 Key Principles

### 4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  Personal data must be processed lawfully, fairly and in a transparent manner. Controllers must provide certain minimum information to data subjects regarding the collection and further processing of their personal data. Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
- **Lawful basis for processing**
  Processing of personal data is lawful only if it is permitted under GDPR, which provides six legal bases on which personal data may be processed. The following are the most relevant for businesses: (i) prior, freely given, specific, informed and unambiguous consent of the data subject; (ii) the processing is necessary for the performance of a contract to which the data subject is a party, or for the purposes of pre-contractual measures taken at the data subject's request; (iii) compliance with legal obligations (i.e., the controller has a legal obligation, under the laws of the EU or an EU Member State, to perform the relevant processing); or (iv) legitimate interests (i.e., the processing is necessary for the purposes of legitimate interests pursued by the controller, except where the controller's interests are overridden by the interests, fundamental rights or freedoms of the affected data subjects). Stronger grounds are required for businesses to process special categories of personal data. It is only permitted under certain conditions, of which the most relevant for businesses are: (i) explicit consent of the affected data subject; (ii) the processing is necessary in the context of employment law; or (iii) the processing is necessary for the establishment, exercise or defence of legal claims.
- **Purpose limitation**
  Data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes are not, in accordance with Article 89(1) of GDPR, considered incompatible with the initial purposes.
- **Data minimisation**
  Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- **Proportionality**
  Data minimisation is the general proportionality principle to be used when deciding how many data to process.
- **Retention**
  As defined in the GDPR under the definition of storage limitation, data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of the data subject.
- *Other key principles – please specify*
  Article 24 of ZVOP-1 is still valid and defines that **data security** must include organisational, technical and logical technical procedures and measures to protect personal data, prevent accidental or deliberate unauthorised destruction of data, their alteration or loss, and unauthorised processing of such data by various measures (protecting premises, preventing unauthorised access to personal data when transmitted, ensuring traceability of any data processing, etc.).
  ZVOP-1 also defines a **prohibition of discrimination** – protection of personal data is guaranteed to every individual irrespective of nationality, race, colour, religion, ethnicity, gender, language, political or other belief, sexual orientation, wealth, birth, education, social status, citizenship, place or type of residence, or any other personal circumstance.

## 5 Individual Rights

### 5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**
  A data subject has the right to obtain from a controller the following information: (i) confirmation of whether, and where, the controller is processing the data subject's personal data; (ii) information about the purposes of the processing;

(iii) information about the categories of data being processed; (iv) information about the categories of recipients with whom the data may be shared; (v) information about the period for which the data will be stored (or the criteria used to determine that period); (vi) information about the existence of the rights to erasure, to rectification, to restriction of processing and to object to processing; (vii) information about the existence of the right to complain to the relevant data protection authority; (viii) where the data were not collected from the data subject, information as to the source of the data; and (ix) information about the existence of, and an explanation of the logic involved in, any automated processing that has a significant effect on the data subject. Additionally, the data subject may request a copy of the personal data being processed.

- **Right to rectification of errors**
  Controllers must ensure that inaccurate or incomplete data are erased or rectified. Data subjects have the right to rectification of inaccurate personal data.
- **Right to deletion/right to be forgotten**
  Data subjects have the right to erasure of their personal data (the "right to be forgotten") if: (i) the data are no longer needed for their original purpose (and no new lawful purpose exists); (ii) the lawful basis for the processing is the data subject's consent, the data subject withdraws that consent, and no other lawful ground exists; (iii) the data subject exercises the right to object, and the controller has no overriding grounds for continuing the processing; (iv) the data have been processed unlawfully; or (v) erasure is necessary for compliance with EU law or national data protection law.
- **Right to object to processing**
  Data subjects have the right to object, on grounds relating to their particular situation, to the processing of personal data where the basis for that processing is either public interest or legitimate interest of the controller. The controller must cease such processing unless it demonstrates legitimate grounds for the processing that overrides the interests, rights and freedoms of the relevant data subject or requires the data in order to establish, exercise or defend legal rights.
- **Right to restrict processing**
  Data subjects have the right to restrict the processing of personal data, which means that the data may only be held by the controller, and may only be used for limited purposes if: (i) the accuracy of the data is contested (and only for as long as it takes to verify that accuracy); (ii) the processing is unlawful and the data subject requests restriction (as opposed to exercising the right to erasure); (iii) the controller no longer needs the data for their original purpose, but the data are still required by the controller to establish, exercise or defend legal rights; or (iv) verification of overriding grounds is pending, in the context of an erasure request.
- **Right to data portability**
  Data subjects have a right to receive a copy of their personal data in a commonly used, machine-readable format and transfer their personal data from one controller to another or, upon the data subject's request, have the data transmitted directly between controllers.
- **Right to withdraw consent**
  A data subject has the right to withdraw their consent at any time. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject must be informed of the right to withdraw consent. It must be as easy to withdraw consent as to give it.
- **Right to object to marketing**
  ZVOP-1, still valid in this part, defines the rights of individuals and obligations of data controllers in Articles 72 and 73 (applicable only for marketing by post). A data controller may use the personal data of individuals that he obtained from publicly accessible sources or within the framework of the lawful performance of activities, as well as for the purposes of offering goods, services, employment or temporary performance of work through the use of postal services, telephone calls, email or other means of telecommunication, unless otherwise provided by another statute. ZVOP-1 also defines the rights of data subjects regarding direct marketing. Individuals may at any time request, in writing or in another agreed manner, that the data controller permanently or temporarily cease to use his personal data for the purpose of direct marketing. The data controller shall be obliged within 15 days to prevent as appropriate the use of personal data for the purpose of direct marketing, and within the subsequent five days to inform in writing or other agreed manner the individual who made such request. An unofficial translation of ZVOP-1 is available here: https://rm.coe.int/16806af30c.
  For email marketing, Article 158 of the ECA is applicable; see section 9 below for further information. An English translation of the law is available here: https://arhiv.akos-rs.si/files/APEK_eng/Legislation/electronic-communications-act-zekom1.pdf.
- **Right to complain to the relevant data protection authority(ies)**
  The national data protection authority is the IC, and for email marketing it is AKOS.
- *Other key rights – please specify*
  There are no other key rights to be discussed.

## 6 Registration Formalities and Prior Approval

**6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?**

Prior to GDPR, controllers were (according to Article 27 of ZVOP-1) obliged to notify the IC about the data filing systems 15 days prior to the establishing of a filing system or prior to the entry of a new type of personal data. Since GDPR entered into force in May 2018, notification is no longer obligatory.

**6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?**

This is not applicable.

**6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?**

This is not applicable.

**6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?**

This is not applicable.

**6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?**

This is not applicable.

**6.6 What are the sanctions for failure to register/notify where required?**

This is not applicable.

**6.7 What is the fee per registration/notification (if applicable)?**

This is not applicable.

**6.8 How frequently must registrations/notifications be renewed (if applicable)?**

This is not applicable.

**6.9 Is any prior approval required from the data protection regulator?**

It is obligatory to get a decision of the IC prior to introduction of any biometric measures. ZVOP-1 is still applicable in this segment; Article 79 for the public sector, and Article 80 for the private sector. The private sector may implement biometric measures only if they are necessarily required for the performance of activities, for the security of people or property, or to protect secret data or business secrets. If the implementation of specific biometric measures in the private sector is not regulated by statute, a data controller intending to implement biometric measures shall, prior to introducing the measures, be obliged to supply the IC with a description of the intended measures and the reasons for the introduction thereof. The IC shall, on receipt of information, be obliged within two months to decide whether the intended introduction of biometric measures complies with ZVOP-1.

ZVOP-1 has a specific regulation regarding linking filing systems (valid only for the public sector), namely Article 84. For Binding Corporate Rules (BCRs), Codes of Conduct and transfer of data to third countries, GDPR applies.

**6.10 Can the registration/notification be completed online?**

This is no longer applicable, although it was possible to notify online in the past.

**6.11 Is there a publicly available list of completed registrations/notifications?**

The old notification register is still available via the following link: https://www.ip-rs.si/varstvo-osebnih-podatkov/register-zbirk.

**6.12 How long does a typical registration/notification process take?**

According to the law, the process should take two months with a possible extension of one additional month; however, in reality it may take up to six months – applicable only for approvals.

## 7 Appointment of a Data Protection Officer

**7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.**

The process is as provided in GDPR. ZVOP-1, still valid in some parts, does not define the obligation to appoint a Data Protection Officer (DPO).

**7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?**

The sanctions are as provided in the GDPR; please note, however, that the IC cannot impose administrative fines until the new Data Protection Act is enacted, and that Slovenia does not recognise administrative fines in supervisory proceedings. The power given to the national data protection authority is to impose misdemeanour fines. As legal grounds are not provided, the IC can only impose fines for the violation of those ZVOP-1 Articles that are still valid.

**7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?**

Yes, and the appointed DPO should not be dismissed or penalised for performing tasks and should report directly to the highest management level of the controller or processor.

**7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?**

A single DPO is permitted by a group of undertakings provided that the DPO is easily accessible from each establishment.

**7.5 Please describe any specific qualifications for the Data Protection Officer required by law.**

The DPO should be appointed based on professional qualities and should have an expert knowledge of data protection law and practices.

**7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?**

The DPO should be involved in all segments of data processing. GDPR outlines the minimum tasks required by the DPO, which include: (i) informing the controller, processor and the relevant employees who process the data of their obligations under GDPR; (ii) monitoring compliance with GDPR, national data protection legislation and internal policies in relation to the processing of personal data including internal audits; (iii) advising on data protection impact assessments and the training of staff; and (iv) co-operating with the data protection authority and acting as the authority's primary point of contact for issues related to data processing.

**7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?**

Yes, the data required to be sent to the IC are: postal address; telephone number; contact email address; and the name of the DPO. Further instructions can be found here: https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebnih-podatkov/klju%C4%8Dna-podro%C4%8Dja-uredbe/poobla%C5%A1%C4%8Dena-oseba-za-varstvo-podatkov#c1910.

**7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?**

The DPO does not need to be named in a public-facing privacy notice. As a matter of good practice, the Article 29 Working Party (now the European Data Protection Board, or EDPB) recommended in its 2017 guidance on DPOs that both the data protection authority and employees should be notified of the name and contact details of the DPO.

## 8 Appointment of Processors

**8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?**

Yes. The business that appoints a processor to process personal data on its behalf is required to sign an agreement with the processor that sets out the subject matter for processing, the duration of processing, the nature and purpose of processing, the types of personal data and categories of data subjects, and the obligations and rights of the controller (i.e., the business). It is essential that the processor appointed by the business complies with GDPR. In June 2020, EDPB approved the Standard Contractual Clauses (SCCs) prepared by the IC.

**8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?**

The processor must be appointed under a binding agreement in writing. The contractual terms must stipulate that the processor: (i) only acts on the documented instructions of the controller; (ii) imposes confidentiality obligations on all employees; (iii) ensures the security of the personal data it processes; (iv) abides by the rules regarding the appointment of sub-processors; (v) implements measures to assist the controller with guaranteeing the rights of data subjects; (vi) assists the controller in obtaining approval from the relevant data protection authority; (vii) either returns or destroys the personal data at the end of the relationship (except as required by EU or Member State law); and (viii) provides the controller with all information necessary to demonstrate compliance with GDPR.

## 9 Marketing

**9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).**

Electronic marketing is defined in Article 158 of the national ECA. There is an obligation to obtain a person's consent prior to sending direct marketing messages (opt-in). There is an exception as defined in the EU ePrivacy Directive and transposed to national law for the emailing of a purchaser of products or services of a legal entity. In such cases, so-called "soft opt-in" is permitted – see paragraph 2 of Article 158 of the ECA.

The use of automated calling and communication systems to make calls to subscribers' telephone numbers without human intervention (e.g., automatic calling machines, SMS, MMS), facsimile machines or email for the purposes of direct marketing is permitted only based on a subscriber's or user's prior consent.

A natural person or legal entity that obtains the email address of a purchaser of its products or services may use that address for the direct marketing of its own similar products or services, on the condition that it gives said customers the clear and distinct opportunity to refuse, free of charge and in a straightforward manner, the use of their email address at the time of the collection of these contact details, and in every subsequent message in the event that the customer has not initially refused such use.

The use of means of direct marketing using electronic communication (e.g., voice calls) is permitted only with the consent of the subscriber or user.

**9.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?**

These restrictions apply only for business-to-consumer marketing with the possibility of using the email address of a person employed by the company to which a marketing message is sent if the address is publicly available on the official website (or on a personal LinkedIn profile) of the company for which the person works. The relevant joint opinion of AKOS and the IC on this topic from 2016 can be found here: https://www.gdpr-guru.eu/blog/blog-5/post/skupno-mnenje-ip-in-akos-o-neposrednem-trzenju-na-sluzbene-e-naslove-7470.

**9.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).**

In general, marketing via telephone is permitted if a person is not listed on a so-called "do not call register". Article 150 of the ECA also provides that subscribers must be given the opportunity to determine whether their personal data are to be included in a public directory, and if so, which data. The issuer of a directory must clearly mark the prohibition applying to the use of a subscriber's personal data for a particular purpose in the directory. Where a subscriber signals a prohibition of use after entry in the directory, or changes the content of that prohibition, the issuer of the directory must enter the change in the next issue of the directory.

**9.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?**

As long as the data subject is in Slovenia, European and other international traders must comply with the Slovenian ECA.

**9.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?**

Yes, AKOS is the relevant data protection authority active in the enforcement of breaches of marketing restrictions.

**9.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?**

No, it is not possible to buy marketing lists from third parties. It is only possible to buy a digital telephone book (on a CD) and, when using the data from it, the controller must respect a decision not to call if the data subject is listed on the "do not call register".

**9.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?**

For mail sent by post as defined in ZVOP-1, the maximum penalty is EUR 4,170 for legal entities and EUR 830 for responsible persons (see Article 93). For violations of Article 158 of the ECA, the maximum penalty is up to EUR 20,000 for legal entities and EUR 500 for responsible persons (see Article 235 of the ECA).

## 10 Cookies

**10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).**

The restrictions are defined in Article 157 of the ECA. Installing of cookies is permitted only upon an individual's consent and clear comprehensive information is requested in advance about the information manager and the purpose of the processing of this information, all in accordance with GDPR. The supervisory body for cookies is the IC.

**10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?**

No, Slovenian legislation does not distinguish between different types of cookies.

**10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?**

Yes, the IC regularly receives complaints and acts accordingly.

**10.4 What are the maximum penalties for breaches of applicable cookie restrictions?**

The maximum penalties are up to EUR 20,000 for legal entities and up to EUR 500 for responsible persons (see Article 234 of the ECA).

## 11 Restrictions on International Data Transfers

**11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.**

If the transfer does not go to an Adequate Jurisdiction, the data exporter should first explore the possibility of implementing one of the safeguards provided for in GDPR before relying on a derogation.

**11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).**

When transferring personal data to a country other than one with Adequate Jurisdiction, businesses must ensure that there are appropriate safeguards on the data transfer, as prescribed by GDPR. GDPR offers several ways to ensure compliance for international data transfers (i.e., consent). Other common options are the use of SCCs or BCRs. After a Court of Justice of the EU decision known as Schrems II (annulment of Privacy Shield), data exporters may still use SCCs. However, the Court of Justice of the EU held that exporters using SCCs must evaluate the legal landscape of the recipient jurisdiction and take any "supplementary measures" necessary to ensure that data are protected at the level required under EU law.

**11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.**

According to ZVOP-1, when using SCCs, the data exporter had to obtain a special decision from the IC permitting the transfer of personal data. However, since the GDPR entered into force, these Articles are no longer valid.

**11.4 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?**

The IC published a press release on 16 November 2020 in which it pointed out the relevant EDBP guidelines on this topic, available in Slovenian via the following link: https://www.ip-rs.si/novice/6051f21930774.

**11.5 What guidance (if any) has/have the data protection authority(ies) issued in relation to the European Commission's revised Standard Contractual Clauses?**

No such guidelines have been issued.

## 12 Whistle-blower Hotlines

**12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?**

There is no legislation applicable for whistle-blower hotlines.

There are some provisions in the Integrity and Prevention of Corruption Act, applicable only for the public sector. Guidelines were written by the Slovenian Commission for the Prevention of Corruption that concern the protection of whistle-blowers. According to the Commission, it is very important that existing resources, institutions, legal mechanisms, and other measures for the protection of human dignity in the work environment and environments where the so-called administrative position is expected to endanger applicants are used in the normative and operational level for protection of whistle-blowers. At European level, Directive (EU) 2019/1937 of the European Parliament and the Council of 23 October 2019 on the protection of persons reporting infringements of Union law should not be overlooked. The said Directive will provide for minimum standards for the protection of applicants, the establishment of channels for reporting and dealing with infringements, and judicial protection for applicants who will receive retaliation. Slovenia must transpose the Directive into national law within two years, or by 17 December 2021. As of June 2021, there has been no concrete news on the progress of its implementation into Slovenian law. There is also a delay in the adoption of the new governmental plan for strengthening integrity and transparency, about which the Ministry of Public Administration said that it has not yet been adopted due to "priorities and activities related to the government's measures to curb the epidemic".

Some additional guidelines for the public sector that concern the organisation of internal pathways to report irregularities are included in the guidelines for the design, implementation and enforcement of the Integrity Plan. The Integrity Plan may also be drawn up by private sector organisations with the assistance of the Commission. For the private sector, the Slovenian Corporate Integrity Guidelines are applicable, which are guidelines for private law companies, formed by the Slovenian Chamber of Commerce, the Manager Association, the Association of Slovenian Supervisors, and members from the Faculty of Economics, University of Ljubljana in 2014.

**12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?**

It is generally permitted to report anonymously. If not reported anonymously, reporters of suspected corruption who act in good faith and who believe that the information they provide to the Commission is true are granted measures to ensure the confidentiality of their identity, as well as protection against retaliation. These elements are also considered by the Commission when assessing the content of the received reports and weighing up whether the reporting persons meet the conditions for protection. Disclosure of the identity of the reporting person is possible based on personal consent or a court order.

## 13 CCTV

**13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?**

For CCTV, no prior approval from the IC is needed; however, ZVOP-1, still valid in this part (see Articles 74 to 77), defines several obligations of a data controller. A public or private sector person that conducts video surveillance must publish a notice to that effect. Such notice must be visible and plainly made public in a manner that enables individuals to acquaint themselves about its implementation at the latest when the video surveillance of them begins.

Besides this general obligation of a controller of CCTV, there are also some specifics regarding CCTV used for access to official office premises and business premises. The public and private sectors may implement video surveillance of access to their official office premises or business premises only if necessary for the security of people or property, for ensuring supervision of entering into or exiting from their official or business premises, or where, due to the nature of the work, there exists a potential threat to employees. The written decision must explain the reasons for the introduction of video surveillance. Video surveillance may only be implemented in a manner that does not show recordings of the interior of residential buildings that do not affect entrances to their premises, or recordings of entrances to apartments. All employees of the controller in the public or private sector working in the premises under surveillance must be informed in writing of the implementation of video surveillance. The filing system shall contain a recording of the individual (an image or sound), and the date and time of entry into and exit from the premises; it may also contain the personal name of the recorded individual, the address of his permanent or temporary residence, employment, the number and data on the type of his personal document, and the reason for entry, if the personal data listed are collected in addition to or through the recording of the video surveillance system. Personal data may be stored for a maximum of one year from their creation and shall then be erased, unless otherwise provided for by statute.

There are also some specifics for CCTV for working areas. It may only be implemented in exceptional cases when necessarily required for the safety of people or property or to protect secret data or business secrets, and where such purpose cannot be achieved by milder means. Video surveillance may only be implemented for those areas where the interests listed in the previous paragraph must be protected. Video surveillance shall be prohibited in work areas outside of the workplace, particularly in changing rooms, lifts and sanitary areas. Employees must be informed in advance in writing prior to the commencement of implementation of video surveillance. Prior to the introduction of video surveillance, the employer shall be obliged to consult the representative trade union of the employer.

**13.2 Are there limits on the purposes for which CCTV data may be used?**

Personal data processed by a video surveillance system can be used only for the defined necessary purposes of CCTV, in line with the data limitation provided by Article 5(1)(b) of the GDPR. The CCTV controller may review the videos only according to the purpose of their collection, meaning that video surveillance footage can therefore only be viewed when an "event" connected to the conditions for the introduction of video surveillance occurs.

When performing (any form of) video surveillance, the data controller must provide all the necessary information in accordance with Article 13 of the GDPR.

The IC has issued many opinions regarding CCTV at work, which can be viewed here: https://www.ip-rs.si/vop?tx_jzgdprdecisions_pi1%5BshowUid%5D=2450&tx_jzgdprdecisions_pi1%5BhighlightWord%5D=videonadzor. An employer is not allowed to regularly and without specific reasons review the videos in which employees are present and thus monitor, for example, their work performance and behaviour. An employer may also not, without sufficient information (for example,

without a sufficiently precise indication of the time period in which a harmful event occurred), review the recordings and thus seek evidence for possible further proceedings. Exceptionally, access to video surveillance footage would be permissible in the event of an extraordinary, deviant event (when the video could possibly also serve as additional evidence in legal proceedings); for example, in the case of specific suspected criminal offences or infringements related to the harmful event that video surveillance footage might cover. In such a case, police are entitled to order a release of the CCTV footage.

## 14 Employee Monitoring

**14.1 What types of employee monitoring are permitted (if any), and in what circumstances?**

CCTV monitoring is permitted as defined in ZVOP-1, and biometric measures can be introduced if permitted by the IC. Any other monitoring is based on a case-by-case decision of the employer, depending mostly on the legitimates interest of the employer who needs to perform a Legitimate Interests Assessment.

**14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.**

No consent is required for monitoring, but for CCTV a prior notice is required. Biometric measures may only be used on employees if they have been informed in writing thereof in advance. The situation when monitoring must be legitimate and should be closely connected to the purpose of monitoring and performed according to ZVOP-1 defined circumstances.

**14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?**

According to ZVOP-1, still valid in this part, consultation is needed prior to implementation of CCTV. For other kinds of monitoring if defined in internal acts, drafts of such acts by which the employer determines the organisation of work or determines the obligations that employees must be aware of in order to fulfil contractual and other obligations, must be submitted to the trade union before being accepted by the employer. The union must give an opinion within eight days.

## 15 Data Security and Data Breach

**15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?**

Anyone processing personal data must implement adequate technical and organisational measures to protect the data against unlawful processing. The obligation is primarily on the controller. In the case that it delegates the processing to a processor, the controller must ensure that the processor guarantees data security. Its obligations must be defined in the controller/processor agreement. Data controllers in the private sector can prescribe in their internal acts the procedures and measures for security of personal data and shall define the persons responsible for individual filing systems and the persons who, due to the nature of their work, shall process individual personal data. Such an act can be an appendix to a controller/processor agreement.

**15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

The controller is responsible for reporting any personal data breach without undue delay (and in any case within 72 hours of first becoming aware of the breach) to the IC unless the breach is unlikely to result in a risk to the rights and freedoms of the data subjects. A processor must notify any data breach to the controller without undue delay. The notification must include the nature of the personal data breach, including the categories and number of data subjects concerned, the name and contact details of the DPO or relevant point of contact, the likely consequences of the breach and the measures taken to address the breach.

**15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

Controllers have a legal obligation to communicate the breach to the data subject without undue delay if the breach is likely to result in a high risk to the rights and freedoms of the data subject. The notification must include the name and contact details of the DPO (or point of contact), the likely consequences of the breach and any measures taken to remedy or mitigate the breach. The controller may be exempt from notifying the data subject if the risk of harm is remote (i.e., because the affected data are encrypted), the controller has taken measures to minimise the risk of harm (i.e., suspending affected accounts) or the notification requires a disproportionate effort (i.e., a public notice of the breach).

**15.4 What are the maximum penalties for data security breaches?**

The IC no longer has powers, as the imposition of administrative fines will be given to the IC with the new national Data Protection Act, planned to be enacted by the end of 2021. However, the IC can impose penalties for lack of data security measures, and ZVOP-1 is still valid in this part. The highest penalty is EUR 12,500 for legal entities and EUR 1,250 for responsible persons (see Articles 24, 25 and 93 of ZVOP-1).

## 16 Enforcement and Sanctions

### 16.1 Describe the enforcement powers of the data protection authority(ies).

| Investigatory/Enforcement Power | Civil/Administrative Sanction | Criminal Sanction |
|---|---|---|
| Investigative Powers | The Information Commissioner (IP) may investigate data processing by private persons on his or her own initiative or at the appeal of a third party. The IP has a wide range of powers to order the controller/processor to provide any information it requires for the performance of its tasks, to conduct investigations in the form of data protection audits, to notify the controller or processor of alleged infringement of the GDPR, to access all personal data and all information necessary and access to the premises of the controller/processor, including any data processing equipment. To use its competencies, the IP can, beside from GDPR, also use the Slovenian Inspections Act (ZIN), which authorises the IP with some more powers (see Article 19 of ZIN). | This is not applicable. |
| Corrective Powers | The IP has a wide range of powers including the ability to issue warnings or reprimands for non-compliance, to order the controller to disclose a personal data breach to the data subject, to impose a permanent or temporary ban on processing and to penalise the controller/processor. | This is not applicable. |
| Authorisation and Advisory Powers | The DPA has a wide range of powers to advise the controller, to authorise the use of biometric measures, contractual clauses and binding corporate rules as outlined in the GDPR. The opinion of the DPA shall be obtained on legislative proposals, executive orders, circulars or similar general regulations that affect the protection of privacy in connection with the processing of personal data.<br>The IP can also advise private persons on data protection issues. | This is not applicable. |
| Imposition of administrative fines for infringements of specified DPA provisions | IP has limited powers at the moment to impose fines, since Slovenia still did not enact a post GDPR Data Protection Act. There are only a few articles in the ZVOP-1, giving IP the power to impose misdemeanour fines. | This is not applicable. |
| Non-compliance with a data protection authority | The Information Commissioner can impose a fine through the misdemeanour procedure on grounds of Inspections Act – see Article 38 of Inspections Act. | This is not applicable. |
| Non-compliance with a data protection authority | The Information Commissioner can impose a fine through the misdemeanour procedure on grounds of Inspections Act – see Article 38 of Inspections Act. | This is not applicable. |

### 16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The IC has that power; no court order is needed.

### 16.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

There have been a number of reactions of the IC connected to unlawful CCTV and abuse of access rights, especially in the public sector. The IC also monitors the COVID-19 vaccination process. In December 2020, the IC initiated an inspection procedure over the implementation of the provisions of ZVOP-1 and GDPR based on a report of suspected excessive processing of personal data of applicants for vaccination against COVID-19 via the e-Administration portal and suspicion of inadequate notification of individuals. None of the three public sector bodies wanted to take the role of controller or the related responsibility for the processing of personal data.

### 16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

No, to the best of our knowledge.

## 17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

### 17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

There is no data collected about this matter, but every business has the obligation to respond and also participate in the legal proceedings that have legal basis in international documents and treaties.

One of such is Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation – the Europol Regulation that regulates data processing for the purposes of: (a) cross-checking aimed at identifying connections or other relevant links between information related to (i) persons who are suspected of having committed or taken part in a criminal offence in respect of which Europol is competent, or who have been convicted of such an offence, or (ii) persons regarding whom there are factual indications or reasonable grounds to believe that they will commit criminal offences in respect of which Europol is competent; (b) analyses of a strategic or thematic nature; (c) operational analyses; and (d) facilitating the exchange of information between Member States, Europol, other Union bodies, third countries and international organisations.

The legal basis for the foreign Law Enforcement Agencies is also the European Convention on Mutual Assistance in Criminal Matters of the Council of Europe. In the EU jurisdiction, Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016, which entered into force in May 2018, should also be considered when providing EU Law Enforcement Agencies with personal data. The Directive protects the fundamental right of citizens to data protection in the use of personal data by law enforcement authorities. This ensures adequate protection of the personal data of victims, witnesses and suspects and facilitates cross-border co-operation in the fight against crime and terrorism.

Problems may arise when the data are requested by a country that is not a Member State of the EU or the Council of Europe and with which Slovenia has not concluded an agreement on mutual legal assistance.

Access to data is usually available through Slovenian judicial authorities and national Law Enforcement Agencies.

### 17.2 What guidance has/have the data protection authority(ies) issued?

No guidance has been issued as of June 2021.

## 18 Trends and Developments

### 18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

Data controllers are regularly fulfilling the obligation under GDPR to notify the IC about data breaches. The IC, after the notification is received, sends a questionnaire about data security and acts accordingly if the answers are not satisfactory. There are still a lot of complaints connected to privacy at work.

### 18.2 What "hot topics" are currently a focus for the data protection regulator?

The IC is constantly following the emergency COVID-19 legislation, as the government often forgets about data protection standards when trying to impose sometimes drastic measures. The IC reacted to a draft law for obligatory COVID-19 application, after which the government removed the obligation and decided to have a decentralised app instead with no obligation for COVID-positive individuals to install it. The IC has also repeatedly pointed out the inadmissible practices of some employers in handling employee emails. As it still detects the presence of such practices when conducting inspection procedures, the IC reminded controllers (employers) in February 2021 to comply with the strict provisions of personal data protection regulations when handling employee emails.

**Nataša Pirc Musar**, Ph.D., graduated from the Faculty of Law of the University of Ljubljana in 1992. From 1989 until 1996, she worked for Slovenian national television as a journalist and news anchor, and from 1996 for five years as a news anchor on "24 ur", the largest commercial television broadcaster in Slovenia, POP TV. In 2003, she became the Director of the Training and Communications Centre of the Supreme Court. From 2004 until 2014, Nataša held the office of Information Commissioner. In 2013, she was elected President of the Europol Joint Supervisory Body. She was also a member of the *ad hoc* EU USA group of experts with the mandate to discuss the "Snowden" affair with the USA. In November 2015, Nataša successfully defended her Ph.D. thesis at the University of Vienna, Austria. She was admitted to the Bar in 2015 and is a President of data protection commission at the Slovenian Bar Association and a Director and Partner at Law Firm PMLS.

**Law Firm Pirc Musar & Lemut Strle Ltd**
Likozarjeva 14
1000 Ljubljana
Slovenia

Tel: +386 1 235 50 30
Email: natasa@pirc-musar.si
URL: www.pirc-musar.si

**Rosana Lemut Strle** graduated from the Faculty of Law of the University of Ljubljana in 1995. In 2002, she passed the state Bar examination, and she finished her post-graduate (LL.M. Master's degree) studies in Ljubljana in 2008. She finished her apprenticeship at an administrative unit in Litija, continued her career in the Municipality of Litija and later became a Chief Legal Officer at the Health Insurance Institute of Slovenia. Rosana joined the Information Commissioner in April 2009, and held the position of Deputy Information Commissioner in charge of personal data protection until December 2014. In January 2015, she became an attorney candidate at Law Firm PMLS, and in February 2016 she was admitted to the Slovenian Bar Association. In March 2016, she became a partner in the law firm. Rosana holds two certificates: CIPP/E (Certified Information Privacy Professional/Europe); and CIPM (Certified Information Privacy Manager).

**Law Firm Pirc Musar & Lemut Strle Ltd**
Likozarjeva 14
1000 Ljubljana
Slovenia

Tel: +386 1 235 50 30
Email: rosana@pirc-musar.si
URL: www.pirc-musar.si

We are a team of seven experienced lawyers led by Nataša Pirc Musar and Rosana Lemut Strle. Nataša Pirc Musar established a law firm in January 2015 shortly after the completion of her 10-year Information Commissioner (IC) mandate, where she gained experience in a wide range of legal fields (the IC is a supervisory body in charge of personal data protection and access to public information). Rosana Lemut Strle was her deputy for six years. Apart from data protection, our law firm also specialises in administrative, labour and media law (criminal cases included) and the whole segment of other civil law fields. We passionately represent clients at court proceedings and are dedicated to high ethical standards.

**www.pirc-musar.si**

Pirc Musar & Lemut Strle
LAW FIRM

# Switzerland



Dr. Gregor Bühler


Luca Dal Molin


Dr. Kirsten Wesiak-Schmidt

Homburger


## 1 Relevant Legislation and Competent Authorities

### 1.1 What is the principal data protection legislation?

In Switzerland, data protection is regulated on the federal and the cantonal level. The Federal Act on Data Protection ("**DPA**") and its corresponding ordinances regulate the processing of personal data by private parties and by federal authorities. In addition, there are cantonal rules addressing the processing of personal data by the cantonal and municipal authorities.

### 1.2 Is there any other general legislation that impacts data protection?

The most important statute regarding data protection is the DPA. There are several implementing regulations and guidelines, such as the Ordinance to the Federal Act on Data Protection and the Ordinance on Data Protection Certification.

### 1.3 Is there any sector-specific legislation that impacts data protection?

Various individual laws contain additional, sector-specific rules on data protection; for instance, in the fields of telecommunication and of research and medicine. For example, the Federal Telecommunications Act contains rules governing the processing of certain personal data by telecommunication service providers, and the Federal Act on Research involving Human Beings contains rules regarding the use of health-related personal data, biological material and genetic data for research purposes.

### 1.4 What authority(ies) are responsible for data protection?

The Federal Data Protection and Information Commissioner ("**FDPIC**") is the federal authority overseeing the application of the DPA. The cantons have their own cantonal data protection authorities for the enforcement of their data protection laws.

## 2 Definitions

### 2.1 Please provide the key definitions used in the relevant legislation:

- "**Personal Data**"
  All information relating to an identified or identifiable natural or legal person.
- "**Processing**"
  Any operation with personal data, irrespective of the means applied and the procedure, and in particular the collection, storage, use, revision, disclosure, archiving or destruction of data.
- "**Controller**"
  This is not expressly defined in Swiss legislation. However, the term is largely interpreted in line with the definition of the EU General Data Protection Regulation ("**GDPR**"), i.e. as the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- "**Processor**"
  This is not expressly defined in Swiss legislation, but the term is largely interpreted in line with the GDPR definition, meaning a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
- "**Data Subject**"
  An individual who is the subject of the relevant personal data. Under current Swiss law, both natural persons and legal entities are considered data subjects and protected by the applicable legislation.
- "**Sensitive Personal Data**"
  Personal data revealing racial origin, political opinions, religious or ideological beliefs, trade-union membership, social security measures, administrative or criminal proceedings or sanctions; data concerning health or the intimate sphere; genetic data; or biometric data.
- "**Data Breach**"
  Not expressly defined in Swiss legislation. However, the term is largely interpreted in line with the GDPR definition, meaning a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised

disclosure of, or access to, personal data transmitted, stored or otherwise processed.

- "**Disclosure**"
  Making personal data accessible, for example by permitting access, transmission or publication.
- "**Data File**"
  Any set of personal data that is structured in such a way that the data is accessible by data subject.
- "**Personality Profile**"
  A collection of data that permits an assessment of essential characteristics of the personality of a natural person.

## 3 Territorial Scope

### 3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The DPA applies to the processing of personal data in Switzerland; i.e., in principle, it does not apply to businesses established elsewhere that do not have Swiss operations. However, the rules of Swiss private international law allow data subjects to choose Swiss law to apply to civil claims under data protection law if there is a sufficient link to Switzerland as provided for in the law (e.g., because the data subject or the controller is established in Switzerland, or because the relevant processing activity takes effect in Switzerland).

## 4 Key Principles

### 4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  This requires that data subjects be informed about the processing of their personal data, unless they have other reasonable means of understanding how their data is processed. When processing sensitive personal data or personality profiles, the data subject needs to be expressly informed about the identity of the data controller, the purpose of the processing and the categories of recipients of such personal data if they are disclosed to third parties.
- **Lawful processing**
  The processing of personal data has to comply with Swiss law. However, contrary to the GDPR, there is no need for a specific legal basis for processing activities.
- **Purpose limitation**
  Personal data may only be processed for the purpose indicated at the time of collection or for the purpose that is evident from the circumstances or provided for by law.
- **Proportionality**
  One may only collect and process such personal data as is necessary to achieve a legitimate purpose, and only as little data and for as long as necessary for pursuing the purpose intended.
- **Good faith**
  One may only process personal data in good faith.
- **Accuracy**
  Personal data must be accurate and, where necessary, kept up to date. Personal data that is incorrect or incomplete in view of the purpose of its processing must not be processed.
- **Data security**
  Those who process personal data have to implement and maintain adequate technical and organisational measures to ensure data security, i.e. to prevent unauthorised processing of such personal data.

If personal data are processed in accordance with these processing principles, data processing is usually considered lawful as long as the data subject has not expressly objected to the relevant processing. The processing of personal data in violation of these principles, and processing notwithstanding the data subject's objection, are considered a breach of the personality rights of the affected data subject. Such breach of personality rights is deemed unlawful unless it can be demonstrated that the processing is justified by the consent of the data subject, by an overriding private or public interest or by a provision of Swiss law.

## 5 Individual Rights

### 5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**
  A data subject may request information on a controller's processing of his or her personal data. In particular, the data subject is entitled to information on: (i) whether the controller processes the data subject's personal data; (ii) the purposes of the processing; (iii) the categories of data that are processed; (iv) the categories of recipients to whom data may be disclosed; and (v) the source of the data. Additionally, the data subject may request a copy of the personal data being processed free of charge. This information right can only be limited or excluded if required by overriding public or, subject to certain limitations, private interests or by a Swiss statutory provision. In practice, courts tend to interpret this right to information broadly, often granting the data subject access to original documents relating to the data subject.
- **Right to rectification of errors**
  Data subjects have the right to rectification of inaccurate personal data.
- **Right to object to processing**
  Data subjects have the right to object to the processing of their personal data, as personal data must not be processed against the data subject's express wishes without justification. The controller may establish a justification for the processing, i.e. a law providing for the processing or an overriding private or public interest. This also results in a right to request deletion of personal data, unless the processor is able to justify the continued retention despite the data subject's request.
- **Monetary compensation**
  If the data subject's personality rights are infringed by unlawful processing of personal data, the data subject may further claim damages, compensation for pain and suffering and disgorgement or profits resulting from the unlawful data processing to the extent it results from the breach of the data subject's personality rights. In practice, however, it is often difficult to prove damage, and Swiss courts are often reluctant to award compensation for pain and suffering.

## 6 Registration Formalities and Prior Approval

### 6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

There is no general legal obligation to register with or notify

the FDPIC of data processing activities. Under certain circumstances, notification or registration obligations may, however, arise. In particular, companies may have to register data files with the FDPIC if they regularly process sensitive personal data or personality profiles, or if they regularly disclose personal data to third parties. The FDPIC maintains a register of data files that are accessible online. Exceptions apply if the processing is required by law or if the company has appointed a data protection officer ("**DPO**"). In addition, there is an obligation to notify the FDPIC with respect to certain cross-border data transfers (*cf.* section 11 below).

**6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?**

The registration of data files has to be made for the specific data file, and contain the information provided for by the DPA.

**6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?**

The registration of data files is made per data file, and per legal entity.

**6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?**

The registration of a data file must be carried out by the person who controls the data file. Usually this is the local Swiss entity.

**6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?**

The registration of data files has to be relatively specific and contain the following information: (i) the name and address of the controller; (ii) the name of the data file; (iii) the person against whom the right of information may be asserted; (iv) the purpose; (v) the categories of personal data processed; (vi) the categories of data recipients; and (vii) the categories of persons participating, i.e. third parties who are permitted to enter and modify data in the data file. This information has to be updated continuously.

**6.6 What are the sanctions for failure to register/notify where required?**

The wilful failure to declare data files, or wilfully providing false information in doing so, is punished by a fine of up to CHF 10,000.

**6.7 What is the fee per registration/notification (if applicable)?**

There is no fee for the registration of a data file.

**6.8 How frequently must registrations/notifications be renewed (if applicable)?**

In principle, the registration is only valid for the specific data file. Thus, a new registration has to be conducted when the facts reported change significantly and it is not sufficient to update the information provided to the register.

**6.9 Is any prior approval required from the data protection regulator?**

As a matter of principle, data files have to be registered before they are opened, but the creating of such data file does not require any approval by the FDPIC.

**6.10 Can the registration/notification be completed online?**

Yes, this can be done online.

**6.11 Is there a publicly available list of completed registrations/notifications?**

The FDPIC maintains a register of data files. It is accessible online and may be viewed by anyone.

**6.12 How long does a typical registration/notification process take?**

The registration of the data file can be completed by filling out an online form.

## 7 Appointment of a Data Protection Officer

**7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.**

There is no legal requirement to appoint a DPO.

**7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?**

This is not applicable.

**7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?**

There are no specific rules for DPOs; the general employment law rules on unfair dismissal apply.

**7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?**

A single DPO is permitted to cover multiple entities.

**7.5 Please describe any specific qualifications for the Data Protection Officer required by law.**

The DPO may be an employee of the controller or a third party. He or she has to be independent, carry out his or her duties without instructions from the controller, and may not carry out any other activities that are incompatible with his or her duties. Moreover, the DPO needs the required specialist knowledge, the resources required and access to all data files and data processing, as well as to all information required to fulfil his or her duties.

**7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?**

A DPO should be involved in all issues which relate to the protection of personal data. The DPA outlines the DPO's minimum responsibilities, which include: (i) auditing the processing of personal data; (ii) recommending corrective measures if data protection regulations are not complied with; (iii) maintaining a list of the data files that are operated by the controller; and (iv) making the list of data files available to the FDPIC or, on request, to data subjects.

**7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?**

In principle, there is no need for such registration or notification. However, if the controller of the data file wishes to be exempted from the duty to register the data file, the FDPIC has to be notified of the appointment of the DPO.

**7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?**

The DPO does not need to be named in the public-facing privacy notice.

## 8 Appointment of Processors

**8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?**

Yes. The processing of personal data may be assigned to third parties by agreement if: (i) the data is processed only in the manner permitted for the instructing party, i.e. the controller, itself; and (ii) it is not prohibited by a statutory or contractual duty of confidentiality. In particular, the instructing party has to ensure that the third party guarantees data security.

**8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?**

The DPA does not state any requirement regarding formalities or issues that have to be addressed. Usually, the agreement is concluded in writing. The controller must ensure that the data are processed only in the manner permitted to the controller, and that data security is guaranteed. GDPR-compliant processor terms can usually be used for Swiss purposes too.

## 9 Marketing

**9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).**

Electronic marketing is regulated by the Federal Act on Unfair Competition ("**UCA**"). It is considered unfair competition to send electronic mass advertising without a direct connection to content requested, without having obtained the prior consent of the customers, indicating the correct sender or pointing to an easy and free-of-charge rejection option. Consent is deemed to be given if contact information has been received from the customer when selling identical or similar goods earlier. In addition, the data protection principles apply to the processing of customers' contact information.

**9.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?**

The above restrictions under the UCA apply to business-to-consumer marketing only.

**9.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).**

In principle, telephone marketing is permitted in Switzerland. Anyone who does not wish to receive promotional calls can register this in the telephone directory with an asterisk (*). According to the UCA, it is considered unfair competition if the notice in the telephone directory that a customer does not wish to receive advertising messages from third parties, and that her or his data may not be passed on for direct marketing purposes, is disregarded. For marketing by post, there are no consent or opt-out requirements. However, a large number of mailboxes in Switzerland have stickers with "no advertising" on them, which means that no marketing communication may be distributed to such mailboxes. In addition, the data protection regulations must always be complied with, including when the contact details are not obtained from public sources.

**9.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?**

The UCA is applicable to all actions affecting the Swiss market due to the principle of impact. For this reason, the regulations also apply to foreign companies that are active on the Swiss market. For the territorial scope of the DPA, please see question 3.1 above.

**9.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?**

No. The State Secretariat for Economic Affairs ("**SECO**") as well as the cantonal prosecution authorities are active in the enforcement of the marketing restrictions set out in the UCA.

**9.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?**

The sale and purchase of contact details is permitted if the data protection regulations are respected on both the buyer and the seller side. In most cases, therefore, the consent of the data subjects will be required to share their contact information with third parties for their marketing purposes.

**9.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?**

The entity that committed the infringement may be sued for damages, satisfaction and surrender of profits; for example, by competitors or customers. Additionally, criminal sanctions can be imposed: natural persons can be punished, on request, for wilfully committing unfair competition, with imprisonment for up to three years or a fine. Under certain circumstances, if the unfair competition is committed while managing the affairs of a legal entity, the representatives can be subject to the same penalty accordingly.

## 10 Cookies

**10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).**

There is no opt-in requirement to use cookies under Swiss law. Website operators, however, have to inform visitors about the use of cookies and similar technologies, including the purpose of the cookies and information about how they can be rejected.

**10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?**

No, Swiss regulation does not distinguish between different types of cookies.

**10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?**

There are no enforcement actions that are publicly known in respect of cookies.

**10.4 What are the maximum penalties for breaches of applicable cookie restrictions?**

A violation of the cookie regulation is considered an administrative offence and can entail a fine of up to CHF 5,000.

## 11 Restrictions on International Data Transfers

**11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.**

Data transfers to jurisdictions that have adequate data protection laws in place are permitted. The transfer of personal data to other jurisdictions is only permitted if adequate data protection is otherwise ensured (e.g., by means of implementing contractual safeguards), or if it or the export can be justified on other grounds (such as consent, the performance of an agreement with the data subject, or the enforcement of a claim in a foreign court).

**11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).**

Frequently, businesses seek to ensure an adequate level of data protection when exporting personal data to a third country by implementing alternative safeguards, including by way of implementing contracts with the data importer. In particular, the EU Model Clauses are acknowledged as sufficient from a Swiss perspective, and so may be used as a contractual basis to transfer personal data to third countries. Alternatively, Binding Corporate Rules ("**BCRs**") can be used for intragroup transfers. Finally, data importers may sign up to the Swiss-US Privacy Shield Framework, which is equivalent to the former EU–US Privacy Shield framework that has been invalidated with the CJEU's *Schrems II* decision. However, while the Swiss-US Privacy Shield Framework is still valid to date, it is unclear how long it may still be used as a basis for data transfers from Switzerland to the USA (*cf.* question 11.4 below).

Aside from such alternative safeguards, businesses may rely on case-by-case justifications. Most importantly, personal data may be transferred to third countries if the data subject has consented, if it is required for executing or performing a contract with the data subject, if it is required to exercise or enforce a right in a foreign court, or if it is justified by overriding public interests.

**11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.**

The FDPIC must be notified if a business wishes to disclose personal data to a third country and it relies on alternative safeguards as a basis for the transfer, such as contractual safeguards or BCRs. Formal approval is not required, but the FDPIC may examine the safeguards and BCRs within 30 days. Once the FDPIC has been notified about the use of specific contractual safeguards or BCRs, the notification duty is deemed fulfilled for all future transfers under the same safeguards. If pre-approved standard contractual clauses (such as the EU Model Clauses) are used, a one-time, general notification about their use is sufficient.

**11.4 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?**

The FDPIC issued a position paper following its annual assessment of the Swiss-US Privacy Shield Framework and the CJEU's decision in the *Schrems II* case. The FDPIC concluded that, although the Swiss-US Privacy Shield Framework guarantees certain protection rights for data subjects in Switzerland, it does not provide an adequate level of protection for data transfers

from Switzerland to the USA under the DPA. However, the FDPIC does not have the authority to invalidate the Swiss-US Privacy Shield Framework.

Furthermore, the FDPIC stated that contractual safeguards such as standard contractual clauses or BCRs cannot prevent access to personal data by foreign authorities, if the public law of the importing country takes precedence and allows official access to the transferred personal data without sufficient transparency and legal protection of the data subjects. Accordingly, the FDPIC assumed that the EU Model Clauses and comparable clauses do not always meet the requirements of contractual safeguards under the DPA for data transfers to jurisdictions without adequate data protection legislation.

**11.5 What guidance (if any) has/have the data protection authority(ies) issued in relation to the European Commission's revised Standard Contractual Clauses?**

The FDPIC has not issued any guidance with respect to the revised EU Model Clauses yet.

## 12 Whistle-blower Hotlines

**12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?**

Whistle-blowing in private businesses is not specifically regulated under Swiss law. Hence, there are no restrictions on the types of issues that may be reported, or on the persons who may submit a report or a concern. Even without a specific law, the processing of personal data by businesses in the context of a whistle-blower scheme is subject to the DPA and employment regulation.

**12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?**

Anonymous reporting is generally permitted.

## 13 CCTV

**13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?**

There is no requirement for separate registration or approval to use CCTV. CCTV, however, has to comply with the DPA, including its requirements regarding transparency and proportionality. Thus, data subjects need to be informed of the use of CCTV before they are captured on camera, e.g., by means of clearly visible signs. Whether or not there is a reasonable need to use CCTV (e.g., security reasons) to render it proportionate is assessed on a case-by-case basis; courts and authorities often take a restrictive view. Where workplaces are covered, relevant employment regulation needs to be complied with.

**13.2 Are there limits on the purposes for which CCTV data may be used?**

There is no general limitation as to the purposes for which CCTV may be used. However, given that the use of CCTV is typically considered to involve high risks for the personality rights of the data subjects, compelling grounds are needed to render it proportionate. This effectively limits the purposes for which its data can be used.

## 14 Employee Monitoring

**14.1 What types of employee monitoring are permitted (if any), and in what circumstances?**

The operation of surveillance or monitoring systems at the workplace is only permitted if the intended purpose cannot be achieved by less restrictive measures. Video surveillance may be permitted for organisational reasons, for security reasons or for production control. In contrast, surveillance systems designed to monitor the behaviour of employees are prohibited.

**14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.**

The employer may only process data about an employee which relate to the employee's suitability for the employment relationship or which are necessary for the execution of the employment contract. Usually, obtaining the employee's consent is not necessary (and such consent may not be a sufficient ground, unless the employee has a real choice to consent or not). However, employees have to be adequately informed about the use and the purpose of the surveillance or monitoring system, and about their right to information.

**14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?**

Employee representatives are entitled to timely and comprehensive information on all matters that they need to be aware of in order to perform their duties. Thus, if such employee representatives exist in a company, it is advisable to keep them informed about employee monitoring. There is, however, no consultation obligation.

## 15 Data Security and Data Breach

**15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?**

Yes. Anyone processing personal data has to implement adequate technical and organisational measures to protect the data against unlawful processing. The obligation is primarily with the controller. In the case that it delegates the processing to a processor, the controller must ensure that the processor guarantees data security.

**15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

The current DPA does not provide for any reporting obligations in the event of data security breaches.

**15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

The current DPA does not provide for any reporting obligations in the event of data security breaches.

**15.4 What are the maximum penalties for data security breaches?**

The current DPA does not provide for specific sanctions for data security breaches; however, the unlawful disclosure of secret information may trigger criminal sanctions.

## 16 Enforcement and Sanctions

**16.1 Describe the enforcement powers of the data protection authority(ies).**

(a) **Investigative Powers**: The FDPIC may investigate data processing by private persons on his or her own initiative or at the request of a third party if:
   (i) methods of processing are capable of breaching the privacy of larger number of persons (system errors);
   (ii) data files must be registered (see section 6 above); or
   (iii) there is a duty to provide information regarding cross-border disclosure of data (see question 11.3 above).

   To this end, the FDPIC may request files, obtain information and arrange for processed data to be shown to him or her.

   Private persons are liable to a fine of up to CHF 10,000 if they wilfully:
   (i) fail to provide information about certain cross-border data transfers;
   (ii) fail to register data files;
   (iii) refuse to cooperate in a case investigation; or
   (iv) provide false information to the FDPIC in doing (i), (ii), or in the course of a case investigation.

   Note that it is not the legal entity that is fined, but the responsible individual.

(b) **Corrective Powers**: On the basis of his or her investigations, the FDPIC may issue a formal recommendation that the method of processing be changed or abandoned.

   If the formal recommendation by the FDPIC is not complied with or is rejected, the FDPIC may refer the matter to the Federal Administrative Court for a decision. The FDPIC has the right to appeal against this decision to the Federal Supreme Court.

(c) **Authorisation and Advisory Powers**: The FDPIC:
   - advises private persons on data protection issues;
   - examines and keeps a list of countries with legislation guaranteeing an adequate level of data protection;
   - examines cross-border transfer of personal data to jurisdictions without an adequate level of data protection on the grounds of model contracts, Standard Contractual Clauses or BCRs (see section 11 above);
   - receives registrations of data files and keeps the register; and
   - examines the certification procedures of independent certification organisations for data processing systems, programmes or organisation, and may issue recommendations.

(d) **Imposition of administrative fines for infringements of specified GDPR provisions**: This is not applicable.

(e) **Non-compliance with a data protection authority**: This is not applicable.

**16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?**

No, the FDPIC does not have the power to ban a particular data processing activity. If a formal recommendation by the FDPIC is not complied with or is rejected, the FDPIC may refer the matter to the Federal Administrative Court to render a binding decision.

**16.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.**

To date, the FDPIC has issued relatively few formal recommendations per year, and even fewer cases have been submitted to the Federal Administrative Court for decision (and ultimately appealed up to the Federal Supreme Court). Recent leading cases were *Helsana+* (2019), *Moneyhouse* (2017), *AXA* and *Google Street View* (2012) and *Logistep* (2010).

**16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?**

Usually, the FDPIC does not exercise its powers against businesses established in other jurisdictions, due to the (in principle) territorial scope of the DPA.

However, in the leading *Google Street View* case, the FDPIC issued a formal recommendation to Google Inc. and Google Switzerland GmbH, collectively, which was submitted to the Federal Administrative Court and ultimately to the Federal Supreme Court for decision. It can be assumed that a judgment would have been enforced primarily against Google Switzerland GmbH, if the Google entities had not complied.

Decisions of Swiss courts regarding businesses established in other jurisdictions would have to be enforced through formal international enforcement procedures.

## 17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

**17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?**

Swiss businesses with an international footprint frequently have to react to foreign e-discovery or data disclosure requests. In doing so, not only data protection law, but also Swiss blocking statutes need to be considered and adhered to. Such blocking

statutes prohibit foreign authorities' activities on Swiss territory as well as the aiding and abetting of such activities. Thus, as a first step, Swiss businesses typically need to verify whether or not they may respond to a foreign request under the blocking statutes. If the foreign request may be complied with in principle, compliance with the DPA needs to be ensured. In this context, the provisions governing cross-border transfers are of particular relevance, including those which permit data exports to exercise or enforce rights in a foreign court.

### 17.2 What guidance has/have the data protection authority(ies) issued?

The FDPIC has issued specific guidance, along the lines set forth above.

## 18 Trends and Developments

### 18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

Under current data protection law, the FDPIC has only limited powers to enforce the DPA, and there are no clear enforcement trends that could be observed over the past 12 months (the last recommendation issued by the FDPIC dates from 2018). The most important topic during the last 12 months was the ongoing revision of the DPA, which will, *inter alia*, grant the FDPIC the power to issue a ban on particular data processing activities. Hence, the FDPIC will have greater enforcement powers under the new law.

### 18.2 What "hot topics" are currently a focus for the data protection regulator?

The FDPIC has recently issued statements regarding a number of data protection questions that arise in the context of measures to fight COVID-19 (such as the use of proximity-tracing apps, the use of telecom provider data to analyse movements and gatherings of people during a lockdown, temperature and health screenings by employers, etc.). After data security concerns became publicly known and a complaint was filed, the FDPIC recently initiated an investigation into the platform "*meineimpfungen*" (and its corresponding mobile application "myViavac") operating the online platform for the Swiss electronic vaccination record. Due to the pending investigation, the online platform went out of business. Similarly, the FDPIC often reviews issues arising in the use of new technology, such as facial recognition, video conferencing, use of cloud technology, social media, etc. It is expected that data protection in the context of the use of technology and digitisation will remain a hot topic over the next 12 months.

Aside from the above, the revision of the DPA, which is expected to enter into force in 2022, will continue to be a key issue.

**Dr. Gregor Bühler** is head of the IP/IT team, and co-heads the Data Protection practice at Homburger. He focuses on intellectual property law, information technology and privacy law. Gregor Bühler represents clients in arbitration and state court proceedings and also acts as arbitrator on IP and technology-related disputes. He is currently Co-Chair of the IBA's Intellectual Property and Entertainment Law Committee. Gregor Bühler completed his legal studies at the University of St. Gallen (*Dr. iur.*) and was admitted to the Bar in 1992. He was a visiting scholar at the Max Planck Institute in Munich (1994–95) and holds a Master's degree (LL.M.) from Georgetown University (1997).

**Homburger AG**
Hardstrasse 201
CH-8005 Zurich
Switzerland

Tel: +41 43 222 1644
Email: gregor.buehler@homburger.ch
URL: www.homburger.ch

**Luca Dal Molin** co-heads the Homburger Data Protection practice. He specialises in data protection and privacy, intellectual property and technology law. He advises clients on all kinds of technology and IT matters, outsourcing projects and IP transactions and he has broad experience in telecommunication law. Luca Dal Molin regularly advises tech companies and supports the implementation of innovative technology and digitalisation strategies. Further, he focuses on copyright, trademark, patent and media law. In all areas of his practice, he represents clients in litigation and regulatory proceedings. Luca Dal Molin studied law at the University of Zurich and graduated in 2008. From 2014 to 2015 he studied at Stanford Law School and obtained a Master of Laws (LL.M.) in Law, Science and Technology.

**Homburger AG**
Hardstrasse 201
CH-8005 Zurich
Switzerland

Tel: +41 43 222 1297
Email: luca.dalmolin@homburger.ch
URL: www.homburger.ch

**Dr. Kirsten Wesiak-Schmidt** is an associate in Homburger's IP/IT and Data Protection teams, and specialises in Swiss and European data protection and privacy, information technology and intellectual property law. She represents clients in litigation and regulatory proceedings in all areas of her practice. Kirsten Wesiak-Schmidt completed her legal studies at the University of Basel (MLaw, *Dr. iur.*) and was admitted to the Bar in 2017. She holds a Master's degree (LL.M.) from Boston University (2014) and is a Certified Information Privacy Professional (CIPP/E).

**Homburger AG**
Hardstrasse 201
CH-8005 Zurich
Switzerland

Tel: +41 43 222 1526
Email: kirsten.wesiak@homburger.ch
URL: www.homburger.ch

# Taiwan


Ken-Ying Tseng


Sam Huang

Lee and Li, Attorneys At Law



## 1 Relevant Legislation and Competent Authorities

### 1.1 What is the principal data protection legislation?

The main statute governing personal data protection in Taiwan is the Personal Data Protection Act ("PDPA"). The Enforcement Rules of the Personal Data Protection Act ("Enforcement Rules") provide further guidelines on interpretation and implementation of the PDPA. The PDPA was first introduced in Taiwan in 1996 and was significantly amended and renamed in 2010, with the amendments becoming effective in 2012. Other than the PDPA and the Enforcement Rules, some central competent authorities have also stipulated the rules with regard to the relevant security matters for the industry sectors under their charge. The framework of the PDPA is similar to that of the privacy legislation of the EU.

### 1.2 Is there any other general legislation that impacts data protection?

The Constitutional Court (consisting of the Justices of the Judicial Yuan) once issued an interpretation which confirmed that the "privacy right" is one of the basic human rights protected under our constitution. Meanwhile, the Civil Code offers general protection on the right to privacy, under which people can bring tort claims for infringement of privacy. Under the Criminal Code and the Communication Protection and Surveillance Act, privacy and secrecy of communications are further protected.

### 1.3 Is there any sector-specific legislation that impacts data protection?

Under the PDPA, central competent authorities have the power to stipulate further rules concerning the "security and maintenance plan for personal information files" and the "disposal measure for personal data after a business ceases operations" for the industry sectors under their charge. For example, the central competent authority in charge of the online retail industry has stipulated such rules for this sector. Some other statutes also stipulate personal data-related matters, such as the Financial Holding Company Act (with regard to cross-selling activities) and the Pharmaceutical Affairs Act (with regard to the Drug Safety Surveillance and Adverse Event Reporting System).

### 1.4 What authority(ies) are responsible for data protection?

The National Development Council ("NDC") is the authority that is currently in charge of interpreting the PDPA. The NDC also acts as a coordinator among different government authorities with regard to the interpretation and implementation of personal data protection matters. The NDC established a Personal Data Protection Office in July 2018 in order to perform the relevant tasks. Another important mission of the Personal Data Protection Office is to obtain the "adequacy decision" from the EU authority concerning the General Data Protection Regulation ("GDPR"). The negotiation commenced in spring 2018.

Meanwhile, central competent authorities and the local (city and county) government authorities are granted the power to enforce certain matters stipulated under the PDPA, such as stipulating rules with regard to the "security maintenance" of personal data, carrying out audits and inspections, and imposing rectification orders and administrative penalties on the non-government agencies they are regulating.

## 2 Definitions

### 2.1 Please provide the key definitions used in the relevant legislation:

- "**Personal Data**"
  The PDPA defines "personal data" as a natural person's name, date of birth, national ID card number, passport number, appearance, fingerprints, marital status, family background, educational background, occupation, contact information, financial status, social activities, sensitive personal data (defined below) and any other information that may be used to directly or indirectly identify a natural person.
- "**Processing**"
  According to the PDPA, "processing" means recording, inputting, storing, editing, correcting, duplicating, indexing, deleting, outputting, linking or internal transmission of personal data for the purpose of setting up or utilising personal information files.
- "**Controller**"
  The PDPA does not use the term "controller" in its text but it adopts similar concepts. Under the PDPA, government and non-government agencies are separately referred to when the text needs to describe the relevant "controller". The PDPA defines a "non-government agency" broadly to include any natural person, juristic person or unincorporated association which is not a government agency.

- "**Processor**"
  Again, the PDPA does not use the term "processor" in its text but it adopts similar concepts. Under the PDPA, when a person/entity collects, processes, and/or uses personal data under the commission or on behalf of others, such a person/entity will be regulated in a way similar to the "processor" being regulated under the GDPR, although with far fewer regulatory burdens.
- "**Data Subject**"
  A "data subject" is a natural person whose personal data is collected, processed, or used.
- "**Sensitive Personal Data**"
  Sensitive personal data include personal data with regard to medical history, medical treatments, genealogy, sex life, health-check results and criminal records.
- "**Data Breach**"
  The PDPA does not use the term "data breach" in its text. The relevant description under the PDPA is an incident under which personal data are stolen, disclosed, altered or infringed in other ways due to a violation of the PDPA by a government or non-government agency.
- "**Indirectly Identifiable**"
  The Enforcement Rules stipulate that whether an individual is "indirectly identifiable" depends on whether or not a government or non-government agency is in possession of or has access to other data, and thereby is able to identify the individual by comparing, combining, or connecting the data collected with such other data.

## 3 Territorial Scope

### 3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The PDPA applies, in principle, to all of the data collection and processing activities taken place in Taiwan without regard to whether the data subjects are Taiwanese nationals or not. The current text of the PDPA does not explicitly provide for the extra-territorial application of the PDPA to offshore entities, although some of its provisions would seem to suggest such an application. The position of the authority has been that the PDPA does not have the type of extra-territorial effect as spelled out under the GDPR, though.

## 4 Key Principles

### 4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  A government or non-government agency is required to notify the data subject of the matters specified under Article 8 or 9 of the PDPA, which in general include: (i) the identity of the government/non-government agency; (ii) the purposes of the collection; (iii) the type of data collected; (iv) the term, place and method of use and the persons who may use the data; (v) the data subject's rights and the manner in which such rights may be exercised; (vi) the consequences of his or her failure to provide the required personal data; and (vii) the source from which the government/non-government agency obtained the personal data (indirect collection).
- **Lawful basis for processing**
  For government agencies, lawful bases for processing include: (i) processing that is provided by law; (ii) having the consent of the data subject; and (iii) processing that will not be detrimental to the rights or interests of the data subject. For non-government agencies, lawful bases for processing include: (i) processing that is provided by law; (ii) having/negotiating a contract between the non-government agency and the data subject, and appropriate security measures having been adopted therefor; (iii) processing of the data that is already in the public domain due to disclosure by the data subject or in a legitimate manner; (iv) processing that is necessary for statistics-gathering or academic research by an academic research institution in the interest of the general public, provided that any information sufficient to identify the data subject has been removed; (v) having the consent of the data subject; (vi) processing that is necessary for the furtherance of public interest; (vii) processing of the data that was collected from publicly available resources, unless the interest of the data subject takes priority over that of the non-government agency; and (viii) processing that will not be detrimental to the rights or interests of the data subject.
  Article 6 of the PDPA prohibits the processing of sensitive personal data unless: (i) processing is provided by law; (ii) processing is necessary for a government agency's performance of its statutory duties or a non-government agency's fulfilment of legal obligations, and appropriate security measures have been or will be adopted therefor; (iii) the data is already in the public domain due to disclosure by the data subject or in a legitimate manner; (iv) processing is necessary for statistics-gathering or academic research by a government agency or academic research institution for medical, health or crime-prevention purpose(s), provided that any information sufficient to identify the data subject has been removed; (v) to the extent necessary to assist a government agency in performing its statutory duties, or a non-government agency in fulfilling legal obligations, and appropriate security measures have been or will be adopted therefor; or (vi) the written consent of the data subject is obtained, provided that processing is still prohibited if the processing goes beyond the necessary extent of specific purpose(s), or any other law prohibits the processing despite the written consent of the data subject, or the consent is obtained against the data subject's will.
- **Purpose limitation**
  To collect personal data, one must have one or more specific purposes and the personal data shall be used within the necessary extent of such purposes. Otherwise, additional legal basis shall be established pursuant to the PDPA.
- **Data minimisation**
  There are no specific data minimisation requirements under the PDPA. However, Article 5 of the PDPA stipulates that the collection, processing, and use of personal data shall not go beyond the necessary extent of the purpose(s) for which the data was collected, and must be reasonably and justifiably related to such purpose(s).
- **Proportionality**
  This is basically the same as data minimisation. Moreover, the PDPA requires a government or non-government agency to have in place appropriate security measures to prevent personal data from being stolen, altered, damaged, destroyed, lost or disclosed. The Enforcement Rules further provide certain technical and organisational measures that a government or non-government agency may consider adopting based on the principle of

proportionality, i.e., based on the quality and quantity of the personal data involved.

- **Retention**
  Neither the PDPA nor the Enforcement Rules prescribe any specific requirements regarding data retention. Nonetheless, the PDPA requires government and non-government agencies to delete or stop collecting, processing or using personal data voluntarily or upon the request of the data subject when the purpose(s) for which the personal data were collected cease(s) to exist or the retention period expires. The retention will be deemed to be necessary for the performance of a government agency's statutory duties or a non-government agency's business operation if: (i) the retention period provided by law or contract has not expired; (ii) the deletion will be detrimental to the rights or interests of the data subject; or (iii) there is any other legal basis for the retention.
- **Other key principles**
  A government or non-government agency must ensure the accuracy of personal data and correct or supplement personal data voluntarily or upon the request of the data subject. If the failure to provide accurate personal data was attributable to a government or non-government agency, it shall notify the persons to whom the data were provided as soon as the government or non-government agency corrects or supplements the data.

## 5 Individual Rights

**5.1 What are the key rights that individuals have in relation to the processing of their personal data?**

- **Right of access to data/copies of data**
  A data subject has the right to access his or her personal data to check and review them and have a copy of the data.
- **Right to rectification of errors**
  A data subject has the right to correct or supplement his or her personal data. A government or non-government agency must cease the processing or use of personal data if there is any dispute over the accuracy of the personal data, unless (i) the processing or use is necessary for the performance of a government agency's statutory duties or a non-government agency's business operation, or (ii) the data subject has given written consent and the dispute has been recorded.
- **Right to deletion/right to be forgotten**
  Whether the right to be forgotten indeed exists under the PDPA is still a subject of debate. However, Article 3 of the PDPA explicitly states that a data subject shall have the right to request a government or non-government agency to delete his/her personal data.
- **Right to object to processing**
  Under the PDPA, there is no "right to object to processing" as defined under the GDPR. However, Article 3 of the PDPA explicitly states that a data subject may request a government or non-government agency to stop processing his/her personal data.
- **Right to restrict processing**
  There is no such right in Taiwan.
- **Right to data portability**
  There is no such right in Taiwan.
- **Right to withdraw consent**
  It is not specified under the PDPA that a data subject may withdraw consent, but a data subject should be able to withdraw consent pursuant to the Civil Code.
- **Right to object to marketing**
  A data subject may object to marketing at any time and a business shall stop any and all marketing activities towards such a data subject at once. Meanwhile, when a non-government agency contacts a data subject for marketing purposes for the first time, the non-government agency shall provide a mechanism for the data subject to object to the marketing free of charge.
- **Right to complain to the relevant data protection authority(ies)**
  This right is not spelled out in black and white under the PDPA but, under the Taiwan legal system, a data subject may always raise a complaint with the relevant competent authorities for any breach of the PDPA.

## 6 Registration Formalities and Prior Approval

**6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?**

There is no such obligation in Taiwan.

**6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?**

This is not applicable.

**6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?**

This is not applicable.

**6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?**

This is not applicable.

**6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?**

This is not applicable.

**6.6 What are the sanctions for failure to register/notify where required?**

This is not applicable.

**6.7 What is the fee per registration/notification (if applicable)?**

This is not applicable.

**6.8 How frequently must registrations/notifications be renewed (if applicable)?**

This is not applicable.

**6.9 Is any prior approval required from the data protection regulator?**

This is not applicable.

**6.10 Can the registration/notification be completed online?**

This is not applicable.

**6.11 Is there a publicly available list of completed registrations/notifications?**

This is not applicable.

**6.12 How long does a typical registration/notification process take?**

This is not applicable.

## 7 Appointment of a Data Protection Officer

**7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.**

The PDPA does not require a non-government agency to appoint a Data Protection Officer. The Enforcement Rules only state that a non-government agency shall allocate "sufficient" manpower to handle personal data protection matters. Hence, it is up to a non-government agency's discretion whether to appoint a Data Protection Officer or not.

**7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?**

This is not applicable.

**7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?**

This is not applicable.

**7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?**

This is not applicable.

**7.5 Please describe any specific qualifications for the Data Protection Officer required by law.**

This is not applicable.

**7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?**

This is not applicable.

**7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?**

This is not applicable.

**7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?**

This is not applicable.

## 8 Appointment of Processors

**8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?**

The PDPA does not mandatorily require a controller to enter into any form of agreement with its processor(s), while the Enforcement Rules require a controller to exercise proper supervision over the processor(s) and suggest certain supervision measures to be taken. As a result, it is advisable for a controller to stipulate such suggested supervision measures in the commission agreement with its processor(s), if any. In addition, for certain industries, such as the pharmaceutical industry, the central competent authority has required that a processing agreement or a similar document setting forth the relevant supervision measures be stipulated.

**8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?**

There is no such formality requirement. Again, it is advisable for a controller to stipulate the below matters in the commission agreement with its processor:

(i) the scope, types, specific purposes and duration of such collection, processing or use;
(ii) the security measures that the processor shall adopt pursuant to the suggested level and scope as set forth under Paragraph 2, Article 12 of the Enforcement Rules;
(iii) whether the processor is allowed to further commission a sub-processor for such processing;
(iv) the specific matters on which the processor must notify the controller, and the remedial measures that must be adopted if the processor or its employee violates the PDPA or relevant regulations;
(v) the matters which are reserved for the controller's further instructions, if any;
(vi) the processor must return all devices containing personal data and delete personal information files stored and kept by the processor due to the performance of such commission agreement when the commission has been terminated or rescinded; and
(vii) the controller shall have the right to periodically check whether the processor carries out the above-mentioned measures.

## 9 Marketing

**9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).**

Sending marketing communications by email or SMS text message to data subjects constitutes use of their personal data. A business may send marketing communications to a data subject by using his or her personal data only if the use is compatible with the specific purpose(s) under which the data was collected, unless the use for any new purpose is legally founded; for example, the data subject has given a separate consent for this new purpose (opt-in rules). A non-government agency must immediately cease the use of personal data for such marketing purposes if the data subject has notified the non-government agency that he or she does not wish to receive such marketing communications (opt-out rules).

**9.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?**

For business-to-business marketing, if no personal data is used – for example, if the marketing communications are sent to a corporate account – the relevant requirements with regard to the use of personal data will not be applicable. In other contexts, more factual situations will need to be evaluated.

**9.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).**

The restrictions are the same as those outlined in question 9.1 above.

**9.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?**

Please see the response to question 3.1 above.

**9.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?**

No, the competent authorities are not very active in this regard.

**9.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?**

No, unless the data subject has specifically consented to such marketing activities; but it is hard to see how such consent could be legally obtained.

**9.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?**

For sending marketing communications without lawful basis for collection, or if the marketing activities are not within the extent of the specific purpose(s) under which the data were collected, a non-government agency may be subject to an administrative fine of up to NT$500,000 and will be ordered to take corrective measures; otherwise, it may be fined consecutively until correction is made.

For failure to comply with the requirement to offer a free opt-out mechanism when a non-government agency contacts a data subject for marketing purposes for the first time, or with the requirement for a non-government agency to stop marketing activities when the data subject raises an objection, the non-government agency will be ordered to take corrective measures within a designated time limit, and may be subject to an administrative fine of up to NT$200,000 if it fails to make corrections.

## 10 Cookies

**10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).**

There is no specific legislation dealing with cookies under Taiwan law. If a non-government agency is able to identify any specific individual by using cookies, the cookies will be deemed "personal data" and the non-government agency shall use the cookies in accordance with the PDPA.

**10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?**

No. The PDPA does not differentiate different types of cookies. As long as they are able to identify individuals, they will be treated as personal data and the one using the cookies shall comply with the PDPA.

**10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?**

No such action has been taken to date.

**10.4 What are the maximum penalties for breaches of applicable cookie restrictions?**

Please see question 16.1.

## 11 Restrictions on International Data Transfers

**11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.**

International data transfers are, in principle, permitted under the PDPA, unless central competent authorities issue any order to prohibit or restrict international data transfers. Under the PDPA, central competent authorities may impose restrictions on a non-government agency's transfer of personal data abroad if: (i) the transfer would prejudice any material national interest; (ii) the transfer is prohibited or restricted under an international treaty or agreement; (iii) the country to which the personal data are to be transferred does not afford sound legal protection of personal data, thereby affecting the rights or interests of the data

subjects; or (iv) the purpose of the transfer is to evade restrictions under the PDPA.

On 25 September 2012, the National Communications Commission ("NCC") issued a blanket order prohibiting communications enterprises (i.e., telecoms carriers and broadcasting operators) from transferring subscribers' personal data to mainland China on the grounds that the personal data protection laws in mainland China are still inadequate.

**11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).**

Businesses will check whether: (i) they have fulfilled their notification obligations to data subjects; (ii) the transfer is compatible with the specified purpose(s); and (iii) they have a lawful basis for the transfer (internal transmission or disclosure to third parties).

**11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.**

No, transfer of personal data to other jurisdictions do not require registration/notification.

**11.4 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?**

This is not applicable.

**11.5 What guidance (if any) has/have the data protection authority(ies) issued in relation to the European Commission's revised Standard Contractual Clauses?**

This is not applicable.

## 12 Whistle-blower Hotlines

**12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?**

Currently, there is not any general whistleblowing legislation under Taiwan law. Nonetheless, a draft Whistleblower Protection Act ("Draft WPA") has been submitted to the Legislative Yuan (i.e., the Congress) for its review. The Draft WPA governs reporting on public servants' non-compliance as well as the whistleblowing mechanism for the private sector. Malpractice in the private sector defined by the Draft WPA includes those types of malpractice that are prescribed as a criminal offence by the Criminal Code and laws with respect to anti-money laundering, labour, finance, government procurement, environmental protection, food safety, medicines, social welfare, etc. Moreover, according to the current proposal, if a business does not respond to a whistleblower's report, the whistleblower may file a report to elected representatives, news media, or public interest groups (two-tiered reporting mechanism). However, it is still uncertain as to whether and when the Legislative Yuan will pass the Draft WPA.

**12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?**

The existing law does not restrict anonymous reporting. The Draft WPA will only provide protection for the individual who discloses his/her identity when making a report. If the individual makes a report without disclosing his/her identity, he/she cannot be protected by the Draft WPA and claim any rights therefrom.

## 13 CCTV

**13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?**

No. However, it is advisable to notify the public by placing a high-visibility sign.

**13.2 Are there limits on the purposes for which CCTV data may be used?**

Unless the CCTV data is recorded in a public place and when the data is used, the recorder does not "tag" or "identify" any individual from the data, the person recording the CCTV data would need to have any of the lawful bases as set forth under Article 19 of the PDPA (please see the response to question 4.1 above) and shall use the CCTV data within the extent of the specific purpose under which the data were collected. Otherwise, consent from the data subject shall be required.

## 14 Employee Monitoring

**14.1 What types of employee monitoring are permitted (if any), and in what circumstances?**

Employee monitoring practices are permitted if (i) the employees no longer have a reasonable expectation of privacy, and (ii) such monitoring is not expressly prohibited by law. Employees are deemed not to have a reasonable expectation of privacy if their employer has expressly announced the monitoring policy and/or employees have consented to the monitoring. Furthermore, employees are deemed to have given an implied consent if they continue to use the equipment provided by the employer after the employer has announced the monitoring policy.

**14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.**

Employers may choose to issue a notice or obtain consent. Typically, employers will expressly announce the monitoring policy by sending emails and/or a written notice to each employee and publishing the monitoring policy at the workplace.

**14.3 To what extent do works councils/trade unions/ employee representatives need to be notified or consulted?**

Only to the extent required under any employment or collective agreement.

## 15 Data Security and Data Breach

**15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?**

The PDPA requires a government or non-government agency to have in place appropriate security measures to prevent personal data from being stolen, altered, damaged, destroyed, lost or disclosed. The Enforcement Rules further provide certain technical and organisational measures that a controller may consider adopting based on the principle of proportionality, i.e., based on the quality and quantity of the personal data involved. A controller is required to supervise the activities of its processor and shall require its processor to adopt appropriate security measures based on the above principles.

**15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

The PDPA does not require the reporting of data breaches to the relevant data protection authorities.

Again, under the PDPA, central competent authorities have the power to stipulate further rules concerning the "security and maintenance plan for personal information files" for the industry sectors under their charge. For example, the central competent authority in charge of the online retail industry has stipulated such rules for this sector and required the relevant business operators to report to the central competent authority any incident which is material and may impact the normal operation of the business or interests of numerous data subjects. There have been quite a few other central competent authorities that have issued similar rules for the industries they regulate, requiring the businesses that they regulate to report data breach incidents to them.

**15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

If there is an incident in which personal data are stolen, leaked, or altered, or the data subjects' interests may otherwise be compromised because of a non-government agency's failure to comply with the PDPA, the non-government agency must notify the data subjects of the incident and the remedies that the non-government agency has adopted as soon as the non-government agency has carried out an investigation of the incident.

**15.4 What are the maximum penalties for data security breaches?**

A non-government agency will be ordered by a data protection regulatory authority to rectify the breach within a time limit prescribed by the authority. If the non-government agency fails to comply with the order within such a time limit, the non-government agency and its statutory representative may each face an administrative fine of up to NT$200,000. They may also be subject to civil liabilities or even criminal liabilities.

## 16 Enforcement and Sanctions

**16.1 Describe the enforcement powers of the data protection authority(ies).**

(a) **Investigative Powers**: Both the central and local government authorities have the power to carry out audits and inspections on non-government agencies. In order to audit and inspect any non-compliance, they may: (i) access the premises of non-government agencies; (ii) require information; and (iii) detain or copy personal data or personal information files that can be confiscated or submitted as evidence. If a non-government agency is found in violation of the PDPA, the authorities may impose an administrative fine and take any of the following actions: (i) prohibit the non-government agency from collecting, processing or using the personal data; (ii) demand the deletion of the personal information files already processed; (iii) confiscate or destroy the personal data illegally collected; and (iv) publicise the violation case, the name of the non-government agency, and the name of the person in charge.

(b) **Corrective Powers**: When the authority finds any non-compliance of the PDPA, the authority has the power to order the private business to take corrective measures as well as imposing administrative fines.

(c) **Authorisation and Advisory Powers: There is no express language under the PDPA setting forth the advisory powers of the relevant competent authorities**. A competent authority may, based on its power of regulating the relevant industry, determine whether to provide consultation or advisory suggestions to the business that it regulates.

(d) **Imposition of administrative fines for infringements of specified GDPR provisions**: GDPR is not applicable in Taiwan. With regard to the PDPA, the competent authorities may impose an administrative fine of between NT$50,000 and NT$500,000 if a non-government agency violates the relevant data protection requirements. Nonetheless, for minor violations such as failure to comply with notification requirements, the competent authority must first designate a time limit for the non-government agency to rectify the failure. Only if the non-government agency fails to rectify the failure within the time limit will the competent authorities impose an administrative fine of between NT$20,000 and NT$200,000. Please note that the administrative fine mentioned above may be imposed consecutively until the violation is rectified, and both the non-government agency and its statutory representative would have an administrative fine of the same amount imposed.

(e) **Non-compliance with a data protection authority**: If a business does not comply with the requirement or order issued by its competent authority, the authority may either resort to the PDPA or the other sectoral regulations to impose fines or other sanctions on the business.

**16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?**

A competent authority may order a private business to stop collecting, processing and using certain personal data if the competent authority deems that such relevant activities are in violation of the PDPA.

**16.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.**

Most cases are related to financial institutions. Several financial institutions have been given administrative fines for breach of confidentiality or unauthorised disclosure of customers' data. In one case, a bank was fined because it failed to take necessary protective measures when uploading its files to a search engine, causing its customers' data to be accessed by the general public online. In the cases involving financial institutions, the Financial Supervisory Commission ("FSC") imposed administrative fines or sanctions in accordance with the law governing the specific industry, such as the Banking Act or the Insurance Act.

**16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?**

No, there have been no such cases thus far.

## 17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

**17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?**

The disclosure and transfer of personal data to foreign law enforcement agencies constitute the use of the personal data for a new purpose, and thus require a valid legal basis for the disclosure (e.g., a use that is specifically permitted by law or based on data subjects' separate consent). Most companies in Taiwan will reject such disclosure unless foreign law enforcement agencies have a Taiwanese court serve the request through judicial assistance, because under those circumstances, such disclosure is permitted by law.

**17.2 What guidance has/have the data protection authority(ies) issued?**

The Taiwan authorities have not issued any guidance in this regard.

## 18 Trends and Developments

**18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.**

There have not been significant enforcement trends in 2020. From time to time, there are some private disputes involving individuals' misuse of government data base (checking government data for private purpose) or unauthorised disclosure of personal data of others (posting personal data of a consumer making complaints on certain public websites).

Meanwhile, the first class action against a private business for a data breach incident was brought to court in March 2018 and it ended up being settled in 2020. The Consumers' Foundation initiated a class action against a famous travel agency for civil compensation on behalf of 25 consumers in 2018. According to the local news, the personal data of around 360,000 customers of the travel agency were compromised by an unidentified source and many of them received calls from phone scammers and suffered losses due to deception. In October 2019, the district court rendered a judgment and dismissed the Consumers' Foundation's claim because of its failure to prove that the travel agency company had committed negligence with regard to adopting appropriate security measures. The Consumers' Foundation filed an appeal against the judgment rendered by the district court and the case was heard in the Taiwan High Court. However, this case was eventually settled by the parties before the Taiwan High Court on July 7, 2020. The travel agency paid the agreed compensation amount in August 2020 and the Consumers' Foundation completed the distribution to the plaintiffs by end of September 2020.

The long-drawn-out "right to be forgotten" lawsuit against Google continues. A manager of a famous professional baseball team was alleged to have been involved in certain fraud cases and scandals, but was not convicted of any crime that was alleged. He changed his name thereafter. However, as long as anyone conducts a search on his name, the relevant news reports concerning the scandals and fraud cases still come up on the screen. This person exercised his right to delete personal data under the PDPA against Google Taiwan and Google LLC. The case against Google Taiwan has been terminated for the reason that Google Taiwan was not responsible for Google's search business in Taiwan. The case against Google LLC was heard by the Taiwan courts. Google LLC claimed that the Taiwan court has no jurisdiction over it because it is not located in Taiwan and that the plaintiff shall not have the right to be forgotten. On February 4, 2021, the Supreme Court overruled the decision of the Taiwan High Court and ordered the case be heard by the Taiwan High Court again. The Supreme Court disagreed with the Taiwan High Court and the Taipei District Court and deemed that it shall be necessary to review carefully again as to whether Google's display of the relevant links to the scandals of the plaintiff shall be deemed within the necessary scope of the usage of the plaintiff's personal data and whether the privacy of the plaintiff shall outweigh the search results given the lapse of time.

With regard to the case brought by certain individuals against our health authority, objecting to our health authority's allowing researchers to access to the data in our National Health Insurance system, such as our medical records, for academic research: previously, our supreme administrative court had opined that the use of data should be deemed legal under the PDPA, and the case was dismissed. The individuals filed an application with the Constitutional Court for further interpretation and, hence, the issue has again become unsettled.

**18.2 What "hot topics" are currently a focus for the data protection regulator?**

In 2020, the Taiwan government announced that it will form a new government agency in charge of the "digital development" of Taiwan. Once, it was stated that the new ministry will be in charge of personal data protection matters, among other

digital-related matters. The Taiwan government announced its plan for the new ministry, the Digital Development Ministry in the end of March 2021 and personal data protection is not among the matters that this new ministry will be in charge of, although it has been understood that the Taiwan government will form or appoint an agency to be in charge of personal data-related matters. Hence, whether there will be a new agency in charge of the personal data matters in Taiwan and whether and how our PDPA will be amended are still under development.

**Ken-Ying Tseng** formed the personal data protection practice at Lee and Li and she currently leads Lee and Li's TMT and Data Privacy Practice Group. She has frequently been invited to deliver speeches or host seminars on digital-related issues, including personal data/privacy, online content regulations, internet governance, AI, blockchain, domain name/IP issues, regulations of large electronic platforms, etc., both in Taiwan and overseas, and has published numerous articles in local and international publications. She regularly advises clients – predominantly multinational companies – on the areas of personal data protection, cybersecurity, artificial intelligence, fintech, OTT, e-payment, P2P lending, sharing economy, domain names, e-signature, Internet security, e-trading, ICP, MOD, cable TV, and satellite TV, as well as other e-commerce or Internet-related matters. Ken-Ying has been repeatedly nominated as an Internet, e-commerce and data protection expert by *Who's Who Legal*, and as a leading individual by other international organisations, such as *Asialaw*, and *IFLR100* among others.

**Lee and Li, Attorneys At Law**
8F, No. 555, Sec. 4, Zhongxiao E. Rd.
Taipei City 11072
Taiwan

Tel: +886 2 2763 8000
Email: kenying@leeandli.com
URL: www.leeandli.com

**Sam Huang** has recently been promoted to a senior associate in 2021. His primary areas of practice include privacy and data protection, e-commerce, TMT, e-payment, e-signature, consumer protection, labour law and general corporate advisory. Sam regularly advises on all aspects of Taiwan privacy and data protection law, from general compliance issues to more specialised and cutting-edge issues.
Prior to joining Lee and Li, Sam served in Deloitte's legal department and the Science & Technology Law Institute ("STLI"), as well as the Institute for Information Industry ("III"). He has extensive experience in assisting the private and public sectors to implement data protection law compliance programmes and conduct data security audits, for industries including construction, real estate brokerage, logistics, hotels, recreation, banking, insurance, as well as government agencies. Sam passed the BS 10012 ("PIMS") lead auditor certification (Certificate No.: ENR-00127314; issued by BSI Taiwan).

**Lee and Li, Attorneys At Law**
8F, No. 555, Sec. 4, Zhongxiao E. Rd.
Taipei City 11072
Taiwan

Tel: +886 2 2763 8000
Email: samhuang@leeandli.com
URL: www.leeandli.com

Lee and Li is a full-service law firm and the largest law firm in Taiwan. Its history can be traced back to the 1940s. Lee and Li has formed practice groups which span corporate and investment, banking and capital markets, trademarks and copyright, patents and technology, and litigation and ADR. Its services are performed by over 100 lawyers admitted in Taiwan and more than 100 technology experts, patent agents, patent attorneys, and trademark attorneys. Lee and Li was recognised as the 'Taiwan Firm of the Year' or the 'National Law Firm of the Year' by *IFLR* from 2001–2020. For its professional and sophisticated legal practice in the field of mergers and acquisitions and financial and capital markets, Lee and Li was named the 'Most Innovative National Law Firm of the Year' for Taiwan in 2019 by *IFLR*. Lee and Li has been recognised by other international institutions as the best law firm in the region, including *Who's Who Legal*, *China Law & Practice*, *Leaders League*, *Chambers and Partners*, and *Asialaw Regional Awards*, among others.

**www.leeandli.com**

# Thailand


Pranat Laohapairoj


Atsushi Okada

Chandler MHM Limited / Mori Hamada & Matsumoto



## 1 Relevant Legislation and Competent Authorities

### 1.1 What is the principal data protection legislation?

The Personal Data Protection Act, B.E. 2562 (2019) ("**PDPA**") is the principal legislation in Thailand. However, the effective date of most parts of the PDPA was recently further postponed for the second time by Royal Decree for another year, and the PDPA will, according to such Royal Decree, be fully effective and enforceable on 1 June 2022.

### 1.2 Is there any other general legislation that impacts data protection?

No, there is not.

### 1.3 Is there any sector-specific legislation that impacts data protection?

There are a few other industry-specific regulations that may touch upon data protection and overlap with the PDPA, such as the regulation governing telecommunication.

### 1.4 What authority(ies) are responsible for data protection?

The Personal Data Protection Committee ("**PDPC**").

## 2 Definitions

### 2.1 Please provide the key definitions used in the relevant legislation:

- "**Personal Data**"
  Any information relating to a natural person, which enables the identification of such person, directly or indirectly, but not including the information of deceased persons.
- "**Processing**"
  There is no definition provided by law.
- "**Controller**"
  A natural or juristic person having the power and duties to make decisions regarding the collection, use or disclosure of Personal Data.
- "**Processor**"
  A natural or juristic person who operates in relation to the collection, use or disclosure of Personal Data pursuant to the orders given by or on behalf of a Controller – such person not being the Controller.
- "**Data Subject**"
  There is no definition provided by law.
- "**Sensitive Personal Data**"
  There is no definition provided by law. However, explicit consent is necessary for collecting Personal Data pertaining to racial or ethnic origin, political opinions, cultic, religious or philosophical beliefs, sexual behaviour, criminal records, health data, disabilities, trade union information, genetic data, biometric data or any data which may affect the data subject in the same manner as prescribed by the PDPC, subject to some exceptions.
- "**Data Breach**"
  There is no definition provided by law.

## 3 Territorial Scope

### 3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The PDPA applies to the collection, use or disclosure of Personal Data of data subjects located in Thailand by businesses in other jurisdictions in the following circumstances:

(1) where the business offers goods or services to data subjects located in Thailand; or
(2) where the business monitors the behaviour of data subjects taking place in Thailand.

## 4 Key Principles

### 4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  The Controller must inform data subjects of the following details prior to or at the time of collecting Personal Data:
  (1) the purpose of the collection, use or disclosure of Personal Data;
  (2) a notification stating that data subjects must provide their Personal Data for compliance with a legal obligation, for the performance of a contract, or to enter into a contract, including notification of the possible effects in cases where data subjects do not provide such Personal Data;

(3) the Personal Data to be collected and the period for which the Personal Data will be retained;
(4) the categories of persons or entities to whom the collected Personal Data may be disclosed;
(5) the information, address and contact channel details of the Controller and, if applicable, of the Controller's representative or Data Protection Officer; and
(6) the data subjects' rights.

- **Lawful basis for processing**
  The Controller shall not process Personal Data without the consent of data subjects, unless:
  (1) it is for a purpose relating to the preparation of historical documents or archives for public interest, or for a purpose relating to research or statistics, in which suitable measures to safeguard data subjects' rights and freedoms are put in place and in accordance with the notification as prescribed by the PDPC;
  (2) it is for preventing or suppressing a danger to a person's life, body or health;
  (3) it is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract;
  (4) it is necessary for the performance of a task carried out in the public interest by the Controller, or it is necessary for the exercising of the official authority vested in the Controller;
  (5) it is necessary for the legitimate interests of the Controller or any natural or juristic persons other than the Controller, except where such interests are overridden by the fundamental rights of the data subject; or
  (6) it is necessary for compliance with a law to which the Controller is subject.
- **Purpose limitation**
  The collection, use or disclosure of Personal Data shall not be conducted in a manner that is different from the purpose previously notified to data subjects, unless data subjects have been informed of such new purpose and the consent is obtained prior to the time of such processing or otherwise permitted by law.
- **Data minimisation**
  The collection of Personal Data shall be limited to the extent necessary in relation to the lawful purpose of the Controller.
- **Proportionality**
  The Personal Data to be collected shall be limited to only those absolutely necessary for fulfilling the purpose outlined to data subjects.
- **Retention**
  The Controller must inform data subjects of the data retention period, prior to or at the time of collecting Personal Data. If it is not possible to specify the retention period, the expected data retention period according to the data retention standard must be specified. The Controller must put in place the examination system for erasure or destruction of Personal Data when the retention period ends, when Personal Data is irrelevant or beyond the purpose necessary for which it has been collected, or when data subjects exercise rights in accordance with the PDPA, subject to some exceptions.

## 5 Individual Rights

### 5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**
  Data subjects have the right to request access to and obtain a copy of their Personal Data. The Controller may reject such request only where it is permitted by law or pursuant to a court order, and where such actions would adversely affect the rights and freedoms of others.
- **Right to rectification of errors**
  The Controller shall ensure that Personal Data remains accurate, up-to-date, complete and not misleading. Where a data subject requests the Controller to act in compliance therewith and the Controller does not take any action regarding such request, the Controller shall record such request together with the reasons for its non-compliance.
- **Right to deletion/right to be forgotten**
  Data subjects have the right to request the Controller to erase or destroy their Personal Data, or anonymise their Personal Data, in cases where one of the following grounds applies:
  (1) such Personal Data is no longer necessary in relation to the purposes for which it was processed;
  (2) data subjects withdraw consent on which the processing is based, and where the Controller has no legal ground for such processing;
  (3) data subjects exercise the right to object to processing of their Personal Data as described below; or
  (4) such Personal Data has been unlawfully collected, used or disclosed.
- **Right to object to processing**
  Data subjects have the right to object to the collection, use or disclosure of their Personal Data under the following circumstances:
  (1) such Personal Data is collected with the exemption to consent requirements, unless the Controller can prove that: (a) there is a compelling legitimate ground for processing such Personal Data; or (b) processing of such Personal Data is carried out for the establishment, compliance or exercise of legal claims, or defence of legal claims;
  (2) such Personal Data is processed for the purpose of direct marketing; or
  (3) such Personal Data is processed for the purpose of scientific, historical or statistic research, unless it is necessary for the performance of a task carried out for reasons of public interest by the Controller.
- **Right to restrict processing**
  Data subjects have the right to request the Controller to restrict the use of their Personal Data in the following circumstances:
  (1) when the Controller is pending an examination process in accordance with the data subjects' request to rectify errors;
  (2) when such Personal Data shall be erased or destroyed, but the data subjects request the restriction of the use of such Personal Data instead;
  (3) when it is no longer necessary to retain such Personal Data for the purposes of such collection, but the data subjects have, by necessity, requested further retention for the purposes of the establishment, compliance or exercise of legal claims, or defence of legal claims; or
  (4) when the Controller is pending verification or pending examination with regard to the data subjects' request to object to processing.

- **Right to data portability**
  Data subjects have the right to receive their Personal Data from the Controller if the processing is based on consent or the performance of contracts. The Controller shall arrange such Personal Data to be in a format which is readable or commonly used by way of automatic tools or equipment, and can be used or disclosed by automated means. Data subjects are also entitled to:
  (1) request the Controller to send or transfer their Personal Data in such formats to other Controllers if it can be done by automatic means; or
  (2) request to directly obtain their Personal Data in such formats that the Controller sends or transfers to other Controllers, unless it is impossible to do so because of technical circumstances.
- **Right to withdraw consent**
  Data subjects may withdraw their consent at any time.
- **Right to object to marketing**
  The law is silent on this point, but based on other provisions, any marketing activity will require its own lawful basis, which arguably can be a legitimate interest in some cases, or consent in other cases.
- **Right to complain to the relevant data protection authority(ies)**
  Data subjects may contact and complain to the authority at will.

## 6 Registration Formalities and Prior Approval

**6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?**

No, there is no such obligation based on the current legislation. However, in an event of a certain serious data breach, the Controller must notify the authority of such breach within 72 hours.

**6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?**

The rules regarding notification in an event of a data breach have not been promulgated.

**6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?**

The rules regarding notification in an event of a data breach have not been promulgated.

**6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?**

The Controller must notify the authority in case of a data breach. However, it is also arguably possible according to the current wording of the law, but still pending the additional rules, that a local agent may do this on behalf of the foreign Controller.

**6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?**

The rules regarding notification in the event of a data breach have not been promulgated.

**6.6 What are the sanctions for failure to register/notify where required?**

The administrative fine for failure to notify the authority in the event of a data breach (and also data subjects in the event of a data breach which has a high possibility of effects on the data subjects) is up to THB 3 million.

**6.7 What is the fee per registration/notification (if applicable)?**

There is no fee in an event of notification for a data breach.

**6.8 How frequently must registrations/notifications be renewed (if applicable)?**

This is not applicable in our jurisdiction.

**6.9 Is any prior approval required from the data protection regulator?**

This is not applicable in our jurisdiction.

**6.10 Can the registration/notification be completed online?**

The rules regarding notification in the event of a data breach have not been promulgated.

**6.11 Is there a publicly available list of completed registrations/notifications?**

As of today, there is no such list. The rules regarding notification in the event of a data breach have not been promulgated.

**6.12 How long does a typical registration/notification process take?**

The rules regarding notification in the event of a data breach have not been promulgated.

## 7 Appointment of a Data Protection Officer

**7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.**

The appointment of a Data Protection Officer is mandatory under the following circumstances:
(1) the Controller or Processor is a public authority as prescribed by the PDPC;

(2) the activities of the Controller or Processor in the collection, use or disclosure of Personal Data require regular monitoring of Personal Data or the system, by reason of having a large number of Personal Data as prescribed by the Committee; or
(3) the core activity of the Controller or Processor is the collection, use or disclosure of sensitive Personal Data (i.e., Personal Data pertaining to racial or ethnic origin, political opinions, cultic, religious or philosophical beliefs, sexual behaviour, criminal records, health data, disabilities, trade union information, genetic data, biometric data, or any data which may affect the data subject in the same manner as prescribed by the PDPC).

**7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?**

The administrative fine is up to THB 1 million.

**7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?**

The Controller or Processor is prohibited from dismissing or terminating the Data Protection Officer's employment as the Data Protection Officer performs his or her duties under the PDPA. In the event that there is any problem when performing the duties, the Data Protection Officer must be able to directly report to the highest management person of the Controller or Processor.

**7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?**

In the event that the Controllers or Processors are in the same affiliated business or are in the same group of undertakings, in order to jointly operate the business or group of undertakings as prescribed by the PDPC, such Controllers or Processors may jointly designate a single Data Protection Officer. In this regard, each establishment of the Controller or Processor in the same affiliated business or in the same group of undertakings must be able to easily contact the Data Protection Officer.

**7.5 Please describe any specific qualifications for the Data Protection Officer required by law.**

It is expected that the PDPC will prescribe and announce the qualifications of the Data Protection Officer by taking into account the knowledge or expertise with respect to the protection of Personal Data.

**7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?**

The Data Protection Officer shall have the following duties:
(1) give advice to the Controller or Processor, including the employees or service providers of the Controller or Processor with respect to compliance with the PDPA;
(2) investigate the performance of the Controller or Processor, including the employees or service providers of the Controller or Processor with respect to the collection, use or disclosure of Personal Data for compliance with the PDPA;
(3) coordinate and cooperate with the PDPC in circumstances where there are problems with respect to the collection, use or disclosure of Personal Data undertaken by the Controller or Processor, including the employees or service providers of the Controller or Processor with respect to compliance with the PDPA; and
(4) keep confidential Personal Data known or acquired in the course of his or her performance of duty under the PDPA.

**7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?**

The Controller and Processor must disclose the information of the Data Protection Officer, including contact address and contact channels, to the PDPC.

**7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?**

The Controller and Processor must disclose the information of the Data Protection Officer, including the contact address and contact channels, to data subjects. Data subjects shall be able to contact the Data Protection Officer with respect to the collection, use or disclosure of their Personal Data and the exercise of rights of data subjects under the PDPA.

## 8 Appointment of Processors

**8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?**

In the circumstance where Personal Data is provided to a Processor, the Controller shall have a data processing agreement with the Processor to ensure that the Processor will follow and comply with its duties under the PDPA and the Controller must take action to prevent the Processor from using or disclosing such Personal Data unlawfully or without authorisation. The Processor may carry out the activities related to processing of Personal Data only pursuant to the instruction given by the Controller, except where such instruction is contrary to laws.

**8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?**

The PDPA does not specifically refer to the formalities of or items to be covered by data processing agreements.

## 9 Marketing

**9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).**

There is no special legislation restricting digital marketing. Depending on the circumstances, direct marketing may require consent, but under some circumstances may be carried out under a legitimate interest basis.

**9.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?**

The law does not make any difference between the two types.

**9.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).**

This is not applicable in our jurisdiction.

**9.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?**

Yes, they do.

**9.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?**

This is yet to be witnessed, as the PDPC has not been officially set up yet. As of the date of this publication, it is also likely that the appointment process will have to be extended as there may be change in the composition of the PDPC from the members originally appointed.

**9.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?**

The purchase of a marketing list must be on a lawful basis, whatever that may be under the specific circumstance.

**9.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?**

The maximum administrative penalty is THB 5 million.

## 10 Cookies

**10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).**

There is no specific legislation focused on cookies. Cookies are treated as a simple collection and processing of Personal Data under the PDPA, so long as they enable the identification of data subjects, whether directly or indirectly.

**10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?**

No, they do not.

**10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?**

As of today, there has been no enforcement, as the law is yet to be fully effective and enforceable.

**10.4 What are the maximum penalties for breaches of applicable cookie restrictions?**

The maximum administrative penalty is THB 5 million.

## 11 Restrictions on International Data Transfers

**11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.**

It is permitted to transfer Personal Data to destination countries or international organisations that have an adequate data protection standard, which will be prescribed by the PDPC.

If the destination country is not designated by the PDPC as having an adequate data protection standard, an international data transfer may be permitted under the following circumstances:

(1) where it is for compliance with the law;
(2) where the consent of data subjects has been obtained, provided that the data subject has been informed of the inadequate Personal Data protection standards of the destination country or international organisation;
(3) where it is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract;
(4) where it is for compliance with a contract between the Controller and other natural or juristic persons for the interests of the data subject;
(5) where it is to prevent or suppress a danger to the life, body or health of the data subject or other persons, when the data subject is incapable of giving consent at such time; or
(6) where it is necessary for carrying out activities in relation to substantial public interest.

Otherwise, the Controller or Processor may transfer Personal Data to a foreign country if the Controller or Processor provides suitable protection measures which enable the enforcement of data subjects' rights, including effective legal remedial measures according to the rules and methods which will be prescribed and announced by the PDPC.

Further, there is a special mechanism applicable to an international data transfer between group companies: in the event that the foreign Controller or Processor has put in place a Personal Data protection policy regarding the transferring of Personal Data, and is in the same affiliated business, or is in the same group of undertakings, in order to jointly operate the business or group of undertakings, an international data transfer is permitted if such policy has been reviewed and certified by the PDPC. However, the criteria of such Personal Data protection policy have not been established yet.

**11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).**

As the supplementary rules are not yet available, the simplest and safest form of basis now is consent or contractual performance.

**11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.**

As the supplementary rules are not yet available, there is no requirement for notification.

**11.4 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?**

As the PDPA is not fully effective and the PDPC has yet to be officially announced in the Gazette, there is none.

**11.5 What guidance (if any) has/have the data protection authority(ies) issued in relation to the European Commission's revised Standard Contractual Clauses?**

As the PDPA is not fully effective and the PDPC has yet to be officially announced in the Gazette, there is none.

## 12 Whistle-blower Hotlines

**12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?**

The law is silent on this, but the general rule is that anyone can submit any complaint to the authority at any time, as an affected data subject or concerned person.

**12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?**

The law is silent on this point, but both types of reports are acceptable.

## 13 CCTV

**13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?**

There is no requirement to register with or notify the authority. However, in general, the collection and processing of Personal Data via CCTV for security purposes will require simple notification to the public (visitors and internal personnel). There is no rule on what form the notice must be in, but the general principle under the PDPA is that notification must be clear, reasonable and visible. As of now, it is generally agreed that a clear sign at the entrance to the premises and a detailed notification in the privacy policy of the premises are sufficient.

**13.2 Are there limits on the purposes for which CCTV data may be used?**

Lacking specific consent, CCTV recordings can only be used for security purposes.

## 14 Employee Monitoring

**14.1 What types of employee monitoring are permitted (if any), and in what circumstances?**

Monitoring that is reasonable and reasonably expected by the employees, and which is not unduly intrusive, can be undertaken.

**14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.**

Monitoring, as long as it abides by the characteristics stated above in question 14.1, can be undertaken under legitimate interest or a contractual performance basis. However, some employers may choose consent to be the basis to increase clarity, but this may mean easy revocation by the employees as well. In either case, proper notification is required, whether in the consent form or in the employee data protection policy.

**14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?**

None. Only the data subjects – in this case the employees – need to be notified.

## 15 Data Security and Data Breach

**15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?**

The Controller and Processor must provide appropriate security measures for preventing unauthorised or unlawful loss, access, use, alteration, correction or disclosure of Personal Data.

**15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

The Controller must notify the PDPC of any Personal Data breach without delay and, where feasible, within 72 hours after having become aware of it, unless such Personal Data breach is unlikely to result in a risk to the rights and freedoms of data subjects. The notification and the exemption from the

notification shall be made in accordance with the rules and procedures which will be set forth by the PDPC.

**15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

If the Personal Data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Controller must also notify the Personal Data breach and the remedial measures to the data subjects without delay. The notification and the exemption from the notification shall be made in accordance with the rules and procedures which will be set forth by the PDPC.

**15.4 What are the maximum penalties for data security breaches?**

The maximum administrative penalty is THB 3 million.

## 16 Enforcement and Sanctions

**16.1 Describe the enforcement powers of the data protection authority(ies).**

(a) **Investigative Powers**: Upon receiving complaints, the PDPA expert committee – a sub-committee appointed by the PDPC, can request for any document or information from any person related to the issue or summon them to give a testimony.
(b) **Corrective Powers**: Before ordering a fine, the PDPA expert committee may request the Controller or the Processor to rectify the violation first.
(c) **Authorisation and Advisory Powers**: Same as (b). The expert committee may issue a warning first before ordering a fine, or simply issue advice for good practices.
(d) **Imposition of administrative fines for infringements of specified GDPR provisions**: The maximum administrative fine under the PDPA is THB 5 million.
(e) **Non-compliance with a data protection authority**: Any person who does not comply with the expert committee's order (as mentioned in (a)) shall be subject to an administrative fine of not more than THB 500,000.

**16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?**

Yes, and a court order is not required.

**16.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.**

To date, there is no precedent case.

**16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?**

There is no precedent case as of today, but in theory the PDPC can attempt to enforce against offshore entities, but whether such enforcement would be fruitful is yet to be seen.

## 17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

**17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?**

There is no law on this, meaning it is up to each business to decide whether compliance is in its best interest.

**17.2 What guidance has/have the data protection authority(ies) issued?**

As of today, no such guidance has been released.

## 18 Trends and Developments

**18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.**

As of today, there are no trends, and it is unclear what trends will emerge in the future.

**18.2 What "hot topics" are currently a focus for the data protection regulator?**

As of today, this point is unclear.

**Pranat Laohapairoj** is a Partner at Chandler MHM Ltd. and has been with the firm since 2012. He has worked with Thai and international clients on merger and acquisition, anti-trust, corporate, anti-corruption, compliance, and data protection, providing advice and services involving due diligence (for merger and acquisition, anti-trust, and data protection), deal structuring, negotiation, contract drafting, deal execution, in-house training and public seminar (for anti-bribery, anti-trust, and data protection), internal misconduct investigation, anti-trust defence, and translation. He regularly works on both domestic Thai deals as well as on cross-border investments, and his experience spans multiple sectors, including oil and gas, mining and metal, automotive and automotive parts and support, manufacturing, wholesale and retail, consumer products, chemical, electronics, real estate and shared space, gaming and information technology, import and export, leasing, land and marine transport, hotel management, heavy machinery and machinery rental, investment and marketing consultancy, recruitment, pharmaceutical and supplements, and food and beverage industries. He is admitted to the Bar of the State of New York.

**Chandler MHM Limited**
36th Floor, Sathorn Square Office Tower
98 North Sathorn Road
Silom, Bangrak, Bangkok 10500
Thailand

Tel: +66 2 009 5000
Email: pranat.l@mhm-global.com
URL: www.chandlermhm.com

**Atsushi Okada** is a Partner in Mori Hamada & Matsumoto's office in Tokyo and is Co-Head of the Firm's Data Security, AI/IoT, Fintech and Healthcare practices. He regularly advises international and domestic companies in various industries on compliance with data protection/privacy regulations, including cross-border personal data transfer, and compliance with data protection laws in Japan, Europe, the U.S. and Asian countries. He has been recognised in Japan in major ranking tables, such as *Chambers Global*, *Chambers Asia-Pacific*, *The Legal 500 Asia Pacific*, *Asialaw Leading Lawyers*, *The Best Lawyers in Japan* and *IAM Patent 1000*.

**Mori Hamada & Matsumoto**
Marunouchi Park Building
2-6-1 Marunouchi
Chiyoda-ku Tokyo 100-8222
Japan

Tel: +81 3 5 220 1821
Email: atsushi.okada@mhm-global.com
URL: www.mhmjapan.com

# Turkey


Okan Or


Ali Feyyaz Gül

SEOR Law Firm

## 1 Relevant Legislation and Competent Authorities

### 1.1 What is the principal data protection legislation?

The Law on Protection of Personal Data, Law No. 6698, ("**DPL**") is the principal legislation with respect to data protection. The DPL was published in the Official Gazette dated April 7, 2016 No. 29677.

### 1.2 Is there any other general legislation that impacts data protection?

Yes, Article 20 of the Turkish Constitution (1982), as amended in 2010, stipulates the right to privacy. According to this Article, everyone is entitled to request protection of his/her Personal Data. This right entails the right to information, right to access, right to request correction or erasure and right to be informed on proper use. Moreover, Articles 135–140 of the Turkish Criminal Code, Law No. 5237, stipulate crimes and penalties related to certain unlawful data Processing cases and failure of erasure of data.

### 1.3 Is there any sector-specific legislation that impacts data protection?

Yes, the Regulation on Processing of Personal Data and Protection of Privacy in the Electronic Communication Sector, and the Regulation on Personal Health Data, are both concentrated on data protection in their respective areas.

In addition, there are a number of pieces of legislation (e.g. in the health and banking sectors) that include provisions on Processing and protection of Personal Data.

These specific provisions supplement the main principles set forth in the DPL and other general legislation.

### 1.4 What authority(ies) are responsible for data protection?

The Personal Data Protection Authority ("**Authority**"), which was established pursuant to the terms of the DPL, is the main authority responsible for data protection. The Personal Data Protection Board ("**Board**") is the decision-making body of the Authority.

## 2 Definitions

### 2.1 Please provide the key definitions used in the relevant legislation:

- "**Personal Data**"
  All kinds of information relating to an identified or identifiable individual.
- "**Processing**"
  Any operation which is performed on Personal Data, wholly or partially by automated means or non-automated means, which forms part of a data filing system, such as collection, recording, storage, protection, alteration, adaptation, disclosure, transfer, retrieval, making available for collection, categorisation, and preventing the use thereof.
- "**Controller**"
  The individual or legal entity who determines the purpose and means of Processing Personal Data and is responsible for establishing and managing the data filing system.
- "**Processor**"
  The individual or legal entity who processes Personal Data on behalf of the Controller upon its authorisation.
- "**Data Subject**"
  The individual whose Personal Data is processed.
- "**Sensitive Personal Data**"
  Personal Data relating to: race or ethnic origin; political opinion; philosophical belief; religion, religious sect or other beliefs; appearance; membership of associations, foundations or trade unions; health; sexual life; criminal convictions and security measures; and biometric and genetic data, are considered to be Personal Data of a special nature (Sensitive Personal Data).
- "**Data Breach**"
  There is no clear definition of "Data Breach" in the DPL. By virtue of Article 12(5) concerning notification of the Board in the event of Data Breaches, it could be concluded that all cases wherein the Processed Personal Data is unlawfully obtained by third parties are considered a Data Breach. However, in the absence of a specific definition, this should not be interpreted in a way that limits the potential scope of Data Breach events.
- "**Data Controller's Representative**" ("**DCR**")
  A Turkish citizen or a Turkish-resident legal entity who is entitled to represent the non-resident Controller before the Authority.

- "**Contact Person**"
  The individual notified to the Registry as the contract person for purposes of communication with the Authority by the Turkish-resident Controller or by the DCR of the non-resident Controller.
- "**Registry**"
  The Data Controllers' Registry, which is organised and kept by the Authority.
- "**VERBIS**"
  The online information system which is developed to enable Controllers to register with and carry out other transactions related to the Registry.
- "**Personal Data Inventory**"
  The Controller's data inventory, which stipulates Processing activities, purpose and legal grounds, data categories, recipient parties, maximum retention period, Personal Data envisaged to be transferred abroad and measures taken for the security of Personal Data.
- "**Personal Data Storage and Destruction Policy**"
  The policy prepared by the Controllers which stipulates the maximum retention period and principles on erasure, destruction and anonymisation of Personal Data.

## 3 Territorial Scope

**3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?**

The DPL does not differentiate with regard to the application of the law between resident and non-resident Controllers. The Authority stated in various decisions, by referring also to the Google Spain Decision of ECJ, that the DPL and its secondary legislation shall apply to non-resident Controllers Processing Personal Data of Data Subjects resident in Turkey.

## 4 Key Principles

**4.1 What are the key principles that apply to the processing of personal data?**

- **Transparency**
  Article 4 of the DPL lists the main principles on Processing of Personal Data. The first main principle is compliance with the law and good faith principle. This broad principle applies to the other principles and is construed to include the requirements of transparent Processing and informing and notifying Data Subjects.
- **Lawful basis for Processing**
  Article 5 of the DPL stipulates the lawful basis for Processing. Apart from obtaining explicit consent of the Data Subject, the exhaustive list of lawful bases for Processing is as follows: (i) express permission by laws; (ii) being mandatory for the protection of physical integrity of the data subject, who is incapable of giving valid consent, or a third person; (iii) necessity related to execution or performance of an agreement; (iv) being mandatory for the Controller's compliance with its legal obligations; (v) having been made public by the Data Subject; (vi) being mandatory for the establishment, exercise or protection of a right; and (vii) provided that it does not violate fundamental rights and freedoms of the Data Subject, being mandatory for the legitimate interests of the Controller.
  Processing of Sensitive Personal Data is subject to stronger conditions. While the main rule is obtaining explicit consent, the other lawful basis varies. If the concerned Sensitive Personal Data relate to health and sexual life, in the absence of explicit consent, Processing can only be carried out by persons or authorised public institutions that have an obligation of confidentiality and for the purposes of protection of public health, operation of preventive medicine, medical diagnosis, treatment and nursing services, planning and management of healthcare services and their financing. If the concerned Sensitive Personal Data are not related to health and sexual life, Processing can be carried out, provided that there is explicit consent, on the lawful basis of express permission by laws.
- **Purpose limitation**
  Processing should be specified, clear and legitimate. The Processing activities should be clearly understandable by the Data Subjects; the lawful basis for Processing Personal Data should be clearly identified; and the Processing activities and their purposes should be specified.
- **Data minimisation**
  Processing should be relevant, limited and proportionate to the purpose of Processing. Accordingly, Controllers should limit Processing activities to those related to the purposes of Processing. Within this scope, Controllers should also avoid Processing for potential future needs, as such would constitute a new Processing activity.
- **Proportionality**
  The Controller should set a reasonable balance between the Processing and the envisaged gain.
- **Retention**
  The Personal Data should be stored for the period set forth in the relevant legislation or the period required for the purpose for which it was Processed. In the absence of a lawful basis for continuing storage, the Personal Data should be erased or anonymised.
- **Accuracy**
  The Processed Personal Data should be accurate and up to date. This is considered to be necessary for the protection of fundamental rights and freedoms of Data Subjects. In parallel with this principle, the DPL stipulates Data Subjects' right to request rectification.

## 5 Individual Rights

**5.1 What are the key rights that individuals have in relation to the processing of their personal data?**

- **Right of access to data/copies of data**
  Individuals have a right to learn whether or not their Personal Data are processed and to request information with respect to the Processing. The Data Subjects are also entitled to learn the purpose of Processing and whether their data are used in accordance with this purpose.
- **Right to rectification of errors**
  Data Subjects may request the rectification of the incomplete or inaccurate data, if any.
- **Right to deletion/right to be forgotten**
  Upon the disappearance of reasons necessitating the Processing, the Personal Data should be erased, destroyed

or anonymised by the Controller *ex officio* or upon request of the Data Subject.

- **Right to object to processing**
  Data Subjects have the right to object to the occurrence of a disadvantageous result against them by the analysis of Processed data through automated systems.
- **Right to restrict processing**
  Not applicable.
- **Right to data portability**
  Not applicable.
- **Right to withdraw consent**
  Data Subjects are entitled to withdraw their consent at any time.
- **Right to object to marketing**
  While the DPL does not specifically provide for the right to object to marketing, the approval of a recipient shall be sought under the Regulation on Electronic Marketing and such approval may be withdrawn by the recipient.
- **Right to complain to the relevant data protection authority(ies)**
  The Data Subject is required to first apply to the Data Controller. If the application is declined, the response is found unsatisfactory or the response is not given in due time, the Data Subject may file a complaint with the Board.
- **Right to information on data transfers**
  The Data Subject is entitled to learn the third persons within or outside Turkey to whom their Personal Data are transferred.
- **Right to damages**
  Apart from the general provisions of law, which may also apply, the DPL stipulates that the Data Subjects are entitled to damages that they have incurred due to unlawful Processing of their Personal Data.

## 6 Registration Formalities and Prior Approval

**6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?**

According to Article 16 of the DPL, businesses that process Personal Data and that are not exempted from the registration requirement are required to be registered with the Registry.

Following multiple postponements, the current deadlines for enrolling in the Registry are as follows:

| Controller | Deadline |
|---|---|
| Controllers whose annual employee number is above 50 or total annual financial statement is above TL 25 million. | December 31, 2021 |
| Controllers who are non-residents. | December 31, 2021 |
| Legal-entity Controllers whose main activity is to process Sensitive Personal Data, and who have an annual employee count below 50 and a total annual financial statement below TL 25 million. | December 31, 2021 |
| Controllers which are state institutions and organisations. | December 31, 2021 |

Additionally, Controllers, who are currently exempt from the registration requirement (e.g. due to total employee number and size of business), would be required to register with the Registry within 30 days, if they lose the exemption.

**6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?**

The definitions of the Processing activities can be general. In fact, Processing activities are picked from the drop-down list in VERBIS, which includes broad descriptions of Processing activities.

**6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?**

The registration is made on the basis of the Controller; each Controller needs to be registered if not exempted.

**6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?**

In principle, all Controllers shall be registered with the Registry. The Board has the authority to make exceptions to this general rule and has introduced a number of group exemptions. For instance, small businesses (fewer than 50 employees and a balance sheet total of below TL 25 million) that are not engaged mainly with Processing Sensitive Personal Data, notaries, lawyers and political parties, among others, are exempted from the registration requirement.

A local branch or subsidiary of a non-resident Controller may require to be registered in addition to the non-resident parent. On the other hand, liaison offices in most cases would not be required to register.

**6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?**

Registration application shall include: (i) identity and address of the Controller and, if any, its DCR; (ii) purposes for which the Personal Data will be processed; (iii) explanations about group(s) of Data Subjects as well as about the data categories belonging to these; (iv) recipients or groups of recipients to whom the Personal Data may be transferred; (v) Personal Data which are envisaged to be transferred abroad; (vi) measures taken for the security of Personal Data; and (vii) maximum retention period.

Also, the Controllers who are obliged to enrol in the Registry are also obliged to prepare a Personal Data Processing Inventory and a Personal Data Storage and Destruction Policy.

**6.6 What are the sanctions for failure to register/notify where required?**

Those who fail to meet the obligations of registration shall be subject to an administrative fine between TL 39,337 and TL 1,966,862 (for the year 2021).

### 6.7 What is the fee per registration/notification (if applicable)?

Enrolment in the Registry is free of charge.

### 6.8 How frequently must registrations/notifications be renewed (if applicable)?

If there are any changes in the registered information, the Controller shall notify the Authority through VERBIS regarding the changes within seven days as of the occurrence of such change.

### 6.9 Is any prior approval required from the data protection regulator?

There is no prior approval process. However, procedurally, a pre-application for registration to VERBIS is made and upon validation by the Authority, an account number is provided to the Controller. The registration procedure may only be commenced upon obtaining this number.

### 6.10 Can the registration/notification be completed online?

Yes, it can be completed online.

### 6.11 Is there a publicly available list of completed registrations/notifications?

Yes. Completed registrations and their content can be searched by the name of Controller from VERBIS.

### 6.12 How long does a typical registration/notification process take?

While registration itself is practical and uploading the necessary information does not take a considerable amount of time, the prior preparation of necessary information and documents may take weeks/months, depending on the Controller.

Typically, the first step for registration is gathering the necessary information to prepare/update the Personal Data Inventory. This may take several weeks depending on the volume of Processing activities and Controller's readiness to pull out and gather necessary information.

In addition, a DCR needs to be appointed for non-resident Controllers. Ideally, the appointment would be made with the resolution of the board/managing body of the Controller, which would be notarised and apostilled. In some cases, this process delays the registration.

## 7 Appointment of a Data Protection Officer

### 7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

Under the DPL, the concept of "Data Protection Officer" does not exist. A comparison can be made with the DCR, whose duties and responsibilities differ, as explained below.

Non-resident Controllers are required to appoint a DCR, as mentioned under question 6.12.

### 7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

There is no specific sanction for failure to appoint a DCR. However, in the absence of a DCR appointment, the non-resident Controller cannot enrol in the Registry, which could trigger the administrative fine mentioned under question 6.6.

### 7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

Compliance with the DPL is the responsibility of the Controller and should be fulfilled by its managing bodies. The DCR's duties relate mostly to practical matters (e.g. ensuring communication with the Authority). Please see question 7.6.

As such, there is no specific protection from disciplinary measures. If the DCR is an employee of the Controller and fails to fulfil its duties, it could be subject to disciplinary measures and employment consequences.

### 7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

There is not any prohibition for a DCR to represent more than one Controller. However, an individual cannot be the Contact Person of more than one Controller.

### 7.5 Please describe any specific qualifications for the Data Protection Officer required by law.

The DCR needs to be a legal entity which is resident in Turkey or a Turkish citizen.

### 7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

The DCR should at least be entrusted with the following powers: (i) to make notification or accept notices or correspondence made by the Authority on behalf of the Controller; (ii) to forward requests directed by the Authority to the Controller, and *vice versa*; (iii) to receive applications to be submitted to the Controller on behalf of the Controller and forward them to the Controller in accordance with the procedure set out by the DCL; (iv) to transmit the response of the Controller to the Data Subjects in accordance with the procedure set out by the DCL; and (v) to carry out transactions and procedures regarding the Registry on behalf of the Controller.

### 7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

A notarised and apostilled copy of the resolution appointing the DCR shall be submitted to the Authority at the time of enrolment in the Registry.

**7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?**

Yes, according to Article 10 of the DPL, the identity of the DCR, if any, should be included in the information notices (or, privacy notices).

## 8 Appointment of Processors

**8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?**

The DPL requires Controllers to take all necessary administrative and technical measures to ensure the security of Personal Data. While entering into an agreement with the Processor is not explicitly required by legislation, it is recommended and could potentially be necessary in order to ensure the security of Personal Data.

The Board's guideline on administrative and technical measures also recommends entering into agreements with Processors.

**8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?**

The Board's guideline on technical and administrative measures recommends execution of a written agreement with the Processor that would cover the following matters: (i) the security measures to be taken; (ii) compliance with the Processing goals and scope, DPL, and data erasure policy; (iii) the confidentiality obligation; (iv) the duty to report any Data Breaches; (v) the Personal Data categories and types transmitted by the Controller to the Processor (if possible); and (vi) the supervision of the systems which store the Personal Data.

## 9 Marketing

**9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).**

The governing pieces of legislation on electronic marketing are the Law on Regulation of Electronic Communication (Law No. 6563) ("Law on E-Communication") and the Regulation on Electronic Marketing.

According to these, principally, commercial electronic messages cannot be sent without the prior consent of the recipient.

In addition, the Regulation on Electronic Marketing envisages a centralised message regulation system ("MRS") to govern the approval, opt-out and complaint mechanisms for commercial electronic messages, and opened for use on January 1, 2021.

**9.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?**

The requirement of prior consent does not apply in a business-to-business context. However, businesses also have the right to reject commercial electronic messages (opt-out), and if they utilise this right, subsequent transmission of messages would require their prior consent.

**9.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).**

There is not a specific restriction for non-electronic marketing (e.g. by post); however, the general provisions of the DPL (e.g. duty to inform, explicit consent for Processing activities, etc.) would apply.

Marketing via any sort of electronic means (e.g. all messages, which includes all data, voice recordings and images sent for commercial purposes via means such as phones, call centres, fax, automated phone call systems, emails, and SMS) would be subject to the Regulation on Electronic Marketing.

**9.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?**

Yes. The Law on E-Communication does not differentiate between marketing sent from Turkey and from other jurisdictions.

**9.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?**

The Ministry of Trade is the responsible body for enforcement of the Regulation on Electronic Marketing.

The Authority is mainly responsible for the enforcement of the DPL and its secondary legislation. In certain decisions, the Authority has resolved that respective breaches of marketing restrictions also violated the DPL and accordingly issued fines.

**9.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?**

For lawful purchase of a marketing list, the relevant individuals should have been duly informed by the seller (such information notice needs to indicate the purchaser) and must have consented to the transfer of their data to the purchaser (unless another lawful basis applies to the specific sale).

In practice, it is recommended that proper due diligence is made on the fulfilment of the duty to inform and receipt of consent. Also, warranties on the legality of the transfer and indemnification of damages could be sought under a written agreement.

**9.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?**

The penalties envisaged under the Law on E-Communication in the event of a breach vary, depending on the rule breached, from TL 2,071 to TL 114,213 (for the year 2021).

The maximum penalty for failure to obtain prior consent is TL 10,381 (for the year 2021), which could be increased tenfold if the failure concerns multiple persons.

## 10 Cookies

**10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).**

There is no specific legislation concerning the use of cookies. To the extent it constitutes Processing, the duties and responsibilities of the Controller under the DPL, such as the duty to inform, would apply to such use.

**10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?**

This is not applicable.

**10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?**

The Authority's decision relating to the Turkish subsidiary of a multinational technology conglomerate was the first enforcement action in relation to cookies. In its decision dated February 27, 2020, the Authority fined the Turkish subsidiary for, among other things, failure to properly inform Data Subjects about Processing through cookies. The Authority did not provide any analysis on cookie types but determined that Processing of Personal Data should be notified (e.g. through pop-ups) to Data Subjects as soon as said Processing begins, and their consent should be obtained, in the absence of another lawful basis for Processing.

**10.4 What are the maximum penalties for breaches of applicable cookie restrictions?**

Please see question 16.1.

## 11 Restrictions on International Data Transfers

**11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.**

Personal Data can be transferred to a foreign jurisdiction if the Data Subjects have provided explicit consent for the transfer.

In its absence, another lawful basis for such Processing (as defined under question 4.1) should be available and:

- the recipient should be in a safe jurisdiction (where Personal Data are sufficiently protected); or
- the Controller in Turkey as well as in the related foreign jurisdiction should provide a written undertaking on the safety of Personal Data, and the authorisation of the Board should have been obtained.

The Authority is yet to announce the list of safe jurisdictions.

**11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).**

Where possible, Controllers aim to obtain explicit consent from Data Subjects for transferring their Personal Data abroad.

**11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.**

Authorisation of the Board is required if the transfer is not based on the explicit consent of the Data Subject and the recipient is not resident in a safe jurisdiction.

The Authority published the minimum content of the undertakings that the Controller needs to provide to obtain the authorisation of the Board. Also, in April 2020, the Authority introduced a "binding corporate rules" procedure as an alternative method for obtaining authorisation on cross-border Personal Data transfers, and published an application form and guidelines on the necessary content of binding corporate rules. This alternative method is envisaged to facilitate the Board's authorisation process for intra-group Personal Data transfers.

**11.4 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?**

Due to its current qualification of all countries as non-safe jurisdictions, the Authority did not issue guidance following the decision of the Court of Justice of the EU in *Schrems II*. Additionally, the Board decided that being a party to Convention No. 108 alone is not sufficient to be qualified as a safe jurisdiction, as mentioned under question 18.1.

**11.5 What guidance (if any) has/have the data protection authority(ies) issued in relation to the European Commission's revised Standard Contractual Clauses?**

No such guidance has been issued.

## 12 Whistle-blower Hotlines

**12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?**

There is no specific legislation addressing corporate whistle-blower hotlines. Under the general provisions of law, businesses can establish their own internal whistle-blower hotlines and determine their scope.

**12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?**

As mentioned above, corporate whistle-blower hotlines are not specifically regulated under law. In compliance with the general provisions of law, businesses can establish hotlines and a procedure for reporting. In line with general corporate governance rules, it is recommended not to prohibit anonymous reporting.

With regard to applications to the Authority, while anonymous reporting is not explicitly allowed or prohibited, the current infrastructure of the complaints mechanism requires

personal information about the complainant, and hence does not allow anonymous complaints.

## 13 CCTV

**13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?**

Use of CCTV is not subject to separate registration, notification or prior approval.

However, it usually constitutes Processing and triggers Controllers' duty to inform. Typically, to comply with the duty to inform, the Controller would have an information notice (privacy notice) available online or in some other location accessible to the Data Subjects, and would have simple signs on the premises which make an initial notification of CCTV recording and identify where the complete information notice can be found. This "informing in stages" approach is also identified as a permissible method in the Board's guidelines.

**13.2 Are there limits on the purposes for which CCTV data may be used?**

There are no specific limitations on purposes for using CCTV data. The general principles of the DPL (e.g. proportionality or lawful basis for Processing) would apply.

Also, as mentioned above, Data Subjects should be duly notified about the collection of their Personal Data and its purposes through the information notice. The actual use of CCTV data should be in compliance with the purposes identified under the information notice.

## 14 Employee Monitoring

**14.1 What types of employee monitoring are permitted (if any), and in what circumstances?**

There are no specific limitations under the DPL.

Under the Labour Law No. 4857 and established precedents of the Court of Appeals, it is considered that the employer may monitor the use of items assigned to employees for work purposes (e.g. emails, computers, cell phones), provided that such monitoring has been made clear to the employees. In the same vein, CCTV recording in common areas is mostly found to be permissible.

The issue has been recently brought before the Constitutional Court of Turkey, which emphasised the balance between the management authority of the employer and fundamental rights of employees, including privacy and communication, and accordingly highlighted and explained the principles of lawfulness, fairness, transparency, purpose limitation, and data minimisation within the context of employee monitoring. The high court also indicated that the employees should be notified of the legal basis and purpose of the Personal Data Processing, its scope, storage period and their rights, possible users of the data and other details of the Personal Data Processing activities due to such monitoring.

**14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.**

As per the Labour Law, the employer shall give notice to employees regarding the scope and clear descriptions of the areas of monitoring.

Within the scope of duty to inform under the DPL, the employer is required to notify all Data Subjects, including employees, about its Processing activities. Such information notices (privacy notices) are typically sent via office email and/or handed over in hard copy along with the signature of the employee confirming receipt.

In most cases, security and operational performance of the business would constitute a lawful basis for Processing (legitimate interest; protection of a right) and explicit consent would not be mandatory.

**14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?**

The rights and duties of work councils, trade unions or employee representatives would be determined pursuant to the Labour Law and its secondary legislation. The DPL does not specify any such requirement.

Generally, if the introduced novelty significantly changes the working conditions to the disadvantage of the employees, the changes need to be accepted by the workers in writing. Likewise, if the envisaged changes contradict the employment agreement or the collective bargaining agreement and require an amendment, the employees or the trade union would need to be notified and agree to the changes.

## 15 Data Security and Data Breach

**15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?**

Yes, the DPL requires Controllers to take all necessary technical and administrative measures to ensure the security of Personal Data.

In the case that the Controller works with a Processor, both the Controller and the Processor would be jointly liable for ensuring the security of Personal Data.

**15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

Yes, in the event of a Data Breach, the Authority should be notified within 72 hours.

Notification shall be made through submission of the Data Breach notification form issued by the Board. Accordingly, to the extent possible, the notification should include details on the type of Data Breach, the time it started/ended/was identified, the causes and consequences of the breach, the total number of affected people and whether they have been informed, the potential results of the breach, and the precautions that were in place and planned to be implemented, among others.

**15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

According to the Board's decision on notification of Data

Breaches, the Controller is required to notify the affected Data Subjects as soon as reasonably possible upon their identification. If possible, the Data Subjects shall be informed of the Data Breach through a direct communication. If not, the Controller shall make the notification through proper means, such as publishing a notification on its website.

**15.4 What are the maximum penalties for data security breaches?**

Those who fail to comply with obligations to ensure the security of Personal Data will be handed an administrative fine of between TL 29,503 and TL 1,966,862 (for the year 2021).

## 16 Enforcement and Sanctions

**16.1 Describe the enforcement powers of the data protection authority(ies).**

(a) **Investigative Powers**: The Board has broad powers to request information and documents from the Controller and, if necessary, to make on-site visits.
(b) **Corrective Powers**: Upon its investigation, the Board may request the Controller to remedy identified violations and order the discontinuation of the Processing.
(c) **Authorisation and Advisory Powers**: The Board is entitled to take and publish generally applicable resolutions to avoid common violations, to determine safe jurisdictions for the transfer of Personal Data abroad and the main methods of administrative and technical measures and to express opinions on draft legislation containing provisions on Personal Data prepared by other institutions and organisations, and to determine the principles of industry-specific implementation, accreditation, certification and training with respect to the protection of Personal Data.
(d) **Imposition of administrative fines for infringements of specified GDPR provisions**: The Board is authorised to issue administrative fines for various violations of provisions. The maximum penalty amount for a single violation is TL 1,966,862 (for the year 2021).
(e) **Non-compliance with a data protection authority**: In case of non-compliance with its resolutions, the Board is authorised to issue administrative fines.

**16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?**

According to Article 15(7) of the DPL, the Board may order the discontinuation of the Processing or transfer of Personal Data to foreign jurisdictions, without a court order, if it concludes that potential damages are irreparable, and the violation is explicit.

**16.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.**

The number of investigations conducted, and resolutions passed by the Board has significantly increased in the last few years. Resolutions have included those with an order for corrective actions, as well as the imposition of fines.

For instance, in a resolution, the Board imposed an administrative fine on the Turkish subsidiary of a worldwide leading online shopping platform due to breach of rules on cross-border transfer and informing Data Subjects. The amount of the administrative fine for the unauthorised cross-border data transfer, which is considered as not taking sufficient security measures, was TL 1.1 million, while the fine was considerably lower, TL 0.1 million, for the breach of rules on informing Data Subjects.

With respect to security measures, the Board recognises a broad interpretation on the scope of measures a Controller needs to take to ensure the security of Personal Data. In another recent case, the Board concluded that the fact that there was a Data Breach shows insufficiency of the Controller's measures and penalised the respective Controller.

The Board is also active on the advisory side. It has made various announcements concerning Personal Data Processing due to health and safety measures related to the COVID-19 Pandemic.

Recently, the Board also published a generally applicable resolution to avoid common violations, especially in the e-commerce, telecommunication, transportation, and tourism sector. The Board recognised the occurrences of accidental transfer of Personal Data to third parties while delivering invoices, due to the failure of Data Subjects in submitting their contact details and highlighted the obligation of the Controller to take reasonable measures to ensure that the Personal Data is accurate and up to date and to evaluate the reliability of the source of the Personal Data.

**16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?**

Yes, the Board has taken resolutions and imposed fines on foreign entities. To our knowledge, there has not been sufficient precedent to test the extraterritorial enforcement capacity of these resolutions.

## 17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

**17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?**

In consideration of commercial interests, businesses are typically helpful in their response to foreign e-discovery requests or requests for disclosure. However, due to the absence of a legal requirement on the Controller, transferring Personal Data to a foreign agency can be problematic and require the explicit consent of the Data Subjects.

**17.2 What guidance has/have the data protection authority(ies) issued?**

No such guidance has been issued.

## 18 Trends and Developments

**18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.**

Generally, the recent investigations of the Board have a focus on compliance with the obligation to inform, rules on cross-border data transfers and obtaining consents for commercial electronic messages. It can be observed that the administrative fines imposed by the Board is higher for breaches of the rules

on cross-border data transfer, which is considered as not taking sufficient measures for the security of the Personal Data.

In the first quarter of 2021, for the first time in its history, the Board made two announcements on grant of authorisation for transfers of Personal Data to other jurisdictions. Considering that there are likely thousands of Controllers that transfer Personal Data abroad, the two authorisation announcements only signal the beginning of the Authority's grant of authorisations.

### 18.2 What "hot topics" are currently a focus for the data protection regulator?

Cross-border transfer of Personal Data continues to be a "hot topic" for the Authority and practitioners of the data protection rules.

The Authority is still expected to issue a list of safe jurisdictions and in its absence considers all jurisdictions as non-safe. This results in a significant increase in the number of authorisation requirements and the authorisation process takes much longer than envisaged, with only two publicly announced grants so far. While these issues are pending, the Board have penalised several Controllers due to unlawful transfer of Personal Data abroad. This problematic situation has led to Turkish government's recent announcement that they consider amending the DPL in order to further harmonise rules on cross-border transfer of Personal Data with the legislation of the European Union.

Another hot topic is the increasing number of decisions published by the Authority regarding commercial electronic messaging. In 2021 the Authority imposed administrative fines on a number of Controllers due to their Processing of Personal Data without consent of Data Subjects and their lack of keeping the Personal Data accurate and up-to-date.

Another pending matter is the absence of legislation or established rules on the method of calculating the exact amount of administrative fines. Under the DPL, administrative fines are determined with wide ranges (in some cases, the maximum amount is 30–50 times the minimum amount). To shed light on the potential consequences of breaches within this wide range, lawmakers and/or the Board are expected to provide further guidance on the determination of administrative fines.

**Okan Or** was admitted to the Istanbul Bar Association in 2008. He was a partner at another leading law firm before co-founding SEOR Law Firm. His main practice areas are mergers & acquisitions, corporate and commercial law, competition, data protection, e-commerce and e-sports. Okan advises clients on a wide range of corporate transactions and has extensive experience in various forms of M&A transaction. He also leads the data protection practice of the firm and has led numerous compliance projects on privacy matters. Okan continues to advise a number of multinational clients and assist their efforts in compliance with local requirements in the area of data protection.

**SEOR Law Firm**
Valikonagi Cad. No: 7 / D:10
Nisantasi 34371
Istanbul
Turkey

Tel: +90 212 251 7272
Email: oor@seor-law.com
URL: www.seor-law.com

**Ali Feyyaz Gül** was admitted to the Istanbul Bar Association in 2018 and has been practising as an associate in the fields of mergers & acquisitions, corporate and commercial law, data protection and e-commerce.

**SEOR Law Firm**
Valikonagi Cad. No: 7 / D:10
Nisantasi 34371
Istanbul
Turkey

Tel: +90 212 251 7272
Email: afgul@seor-law.com
URL: www.seor-law.com

SEOR Law Firm is a boutique law firm located in Istanbul, Turkey. The core disciplines of the firm presently include commercial, corporate and M&A, competition, data privacy, employment, dispute resolution, intellectual property and real estate.
SEOR Law Firm focuses on and pays special attention to partner involvement in all projects, whether large-scale or otherwise. Combining tailored and client-oriented solutions as a boutique law firm with a comprehensive and inter-continental academic and professional background, SEOR is one of the very few law firms that can provide such distinguished law consultancy and service. In addition, SEOR Law Firm's motto is to provide not simply the best legal solutions, but rather a combination of the best legal and business solutions that will benefit the client.

**www.seor-law.com**

SEOR
LAW FIRM

# United Kingdom


Tim Hickman


Joe Devine

White & Case LLP



## 1 Relevant Legislation and Competent Authorities

### 1.1 What is the principal data protection legislation?

Until the UK's departure from the EU, and the end of the 'Transition Period' on 31 December 2020, the principal data protection legislation in the UK was Regulation (EU) 2016/679 (the "**General Data Protection Regulation**" or "**GDPR**"). The GDPR repealed Directive 95/46/EC (the "**Data Protection Directive**") and led to increased (though not total) harmonisation of data protection law across the EU Member States. Some provisions in the GDPR can be adapted in EU Member States' national laws. Therefore, the UK Government passed the Data Protection Act 2018, and several subsequent amendments (the "**DPA 2018**"), which covers those areas of the GDPR which EU Member States could add to or vary or that do not fall within EU law. The DPA 2018 came into force on 25 May 2018.

Following the UK's departure from the EU, the GDPR was incorporated into the domestic law that applies in the UK, under section 3 of the European Union (Withdrawal) Act 2018 (the "**Withdrawal Act**"), and the DPA 2018, as amended by the Data Protection, Privacy and Electronic Communications (Amendments, etc.) (EU Exit) Regulations 2019. The amended GDPR (the "**UK GDPR**") and the DPA 2018 are now the principal pieces of data protection legislation in the UK.

The UK GDPR is broadly aligned with the GDPR in terms of its substantive requirements. However, provisions concerning supervisory bodies and interactions between EU Member States have been amended to reflect the fact that the UK is no longer directly subject to EU law and enforcement regimes. Powers previously held at Union level are now held by the UK's Information Commissioner.

References to 'UK GDPR' used throughout this chapter should be read to include 'DPA 18'.

### 1.2 Is there any other general legislation that impacts data protection?

The Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended from time to time) (the "**PECR**") implement the requirements of Directive 2002/58/EC (as amended by Directive 2009/136/EC) (the "**ePrivacy Directive**"), which provides a specific set of privacy rules to harmonise the processing of personal data by the telecoms sector. The PECR remain in force following the UK's departure from the EU.

In January 2017, the European Commission published a proposal for an ePrivacy regulation (the "**ePrivacy Regulation**") that would harmonise the applicable rules across the EU. In September 2018, the Council of the European Union published proposed revisions to the draft. Subsequent revisions continued to be proposed throughout the course of 2019 and 2020, and on 10 February 2021, the General Secretariat of the Council of the European Union published its full set of amendments. The ePrivacy Regulation is now moving through the EU's legislative process. If adopted, the ePrivacy Regulation will not apply automatically in the UK. However, it is possible that the UK will adopt similar legislation that is broadly aligned with the EU ePrivacy Regulation.

### 1.3 Is there any sector-specific legislation that impacts data protection?

No, there is no sector-specific legislation that impacts data protection.

### 1.4 What authority(ies) are responsible for data protection?

The Information Commissioner's Office (the "**ICO**") is responsible for overseeing and enforcing the UK GDPR and the PECR in the UK. It is an independent body, which is sponsored by the Department for Digital, Culture, Media and Sport and reports directly to Parliament. In July 2016, Elizabeth Denham, CBE was appointed Information Commissioner.

## 2 Definitions

### 2.1 Please provide the key definitions used in the relevant legislation:

- "**Personal Data**"
  Any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- "**Processing**"
  Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording,

organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

- "**Controller**"
  The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- "**Processor**"
  A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
- "**Data Subject**"
  An individual who is the subject of the relevant personal data.
- "**Sensitive Personal Data**"
  Sometimes referred to as "special categories of personal data" under the UK GDPR. This includes personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health or sex life and sexual orientation, genetic data or biometric data.
- "**Data Breach**"
  A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

## 3 Territorial Scope

### 3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The UK GDPR applies to businesses that are established in the UK, and that process personal data (either as a controller or processor, and regardless of whether or not the processing takes place in the UK) in the context of that establishment.

A business that is not established in the UK, but is subject to the laws of the UK by virtue of public international law, is also subject to the UK GDPR.

The UK GDPR applies to businesses outside the UK if they (either as controller or processor) process the personal data of UK residents in relation to: (i) the offering of goods or services (whether or not in return for payment) to UK residents; or (ii) the monitoring of the behaviour of UK residents (to the extent that such behaviour takes place in the UK).

## 4 Key Principles

### 4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  Personal data must be processed lawfully, fairly and in a transparent manner. Controllers must provide certain minimum information to data subjects regarding the collection and further processing of their personal data. Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
- **Lawful basis for processing**
  Processing of personal data is lawful only if, and to the extent that, it is permitted under UK data protection law. The UK GDPR provides an exhaustive list of legal bases on which personal data may be processed, of which the following are the most relevant for businesses: (i) prior, freely given, specific, informed and unambiguous consent of the data subject; (ii) contractual necessity (i.e., the processing is necessary for the performance of a contract to which the data subject is a party, or for the purposes of pre-contractual measures taken at the data subject's request); (iii) compliance with legal obligations (i.e., the controller has a legal obligation, under the laws of the UK, to perform the relevant processing); or (iv) legitimate interests (i.e., the processing is necessary for the purposes of legitimate interests pursued by the controller, except where the controller's interests are overridden by the interests, fundamental rights or freedoms of the affected data subjects).
  Please note that businesses require stronger grounds to process sensitive personal data. The processing of sensitive personal data is only permitted under certain conditions, of which the most relevant for businesses are: (i) explicit consent of the affected data subject; (ii) the processing is necessary in the context of employment law; or (iii) the processing is necessary for the establishment, exercise or defence of legal claims.
- **Purpose limitation**
  Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes. If a controller wishes to use the relevant personal data in a manner that is incompatible with the purposes for which they were initially collected, it must: (i) inform the data subject of such new processing; and (ii) be able to rely on a lawful basis as set out above.
- **Data minimisation**
  Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed. A business should only process the personal data that it actually needs to process in order to achieve its processing purposes.
- **Retention**
  Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- **Accuracy**
  Personal data must be accurate and, where necessary, kept up-to-date. A business must take every reasonable step to ensure that personal data that are inaccurate are either erased or rectified without delay.
- **Data security**
  Personal data must be processed in a manner that ensures appropriate security of those data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- **Accountability**
  The controller is responsible for, and must be able to demonstrate, compliance with the data protection principles set out above.

## 5 Individual Rights

### 5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**
  A data subject has the right to obtain from a controller the following information in respect of the data subject's

personal data: (i) confirmation of whether, and where, the controller is processing the data subject's personal data; (ii) information about the purposes of the processing; (iii) information about the categories of data being processed; (iv) information about the categories of recipients with whom the data may be shared; (v) information about the period for which the data will be stored (or the criteria used to determine that period); (vi) information about the existence of the rights to erasure, to rectification, to restriction of processing and to object to processing; (vii) information about the existence of the right to complain to the relevant data protection authority; (viii) where the data were not collected from the data subject, information as to the source of the data; and (ix) information about the existence of, and an explanation of the logic involved in, any automated processing that has a significant effect on the data subject.

Additionally, the data subject may request a copy of the personal data being processed.

- **Right to rectification of errors**
  Controllers must ensure that inaccurate or incomplete data are erased or rectified. Data subjects have the right to rectification of inaccurate personal data.
- **Right to deletion/right to be forgotten**
  Data subjects have the right to erasure of their personal data (the "right to be forgotten") if: (i) the data are no longer needed for their original purpose (and no new lawful purpose exists); (ii) the lawful basis for the processing is the data subject's consent, the data subject withdraws that consent, and no other lawful ground exists; (iii) the data subject exercises the right to object, and the controller has no overriding grounds for continuing the processing; (iv) the data have been processed unlawfully; or (v) erasure is necessary for compliance with UK law.
- **Right to object to processing**
  Data subjects have the right to object, on grounds relating to their particular situation, to the processing of personal data where the basis for that processing is either public interest or legitimate interest of the controller. The controller must cease such processing unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the relevant data subject or requires the data in order to establish, exercise or defend legal rights.
- **Right to restrict processing**
  Data subjects have the right to restrict the processing of personal data, which means that the data may only be held by the controller, and may only be used for limited purposes if: (i) the accuracy of the data is contested (and only for as long as it takes to verify that accuracy); (ii) the processing is unlawful and the data subject requests restriction (as opposed to exercising the right to erasure); (iii) the controller no longer needs the data for their original purpose, but the data are still required by the controller to establish, exercise or defend legal rights; or (iv) verification of overriding grounds is pending, in the context of an erasure request.
- **Right to data portability**
  Data subjects have a right to receive a copy of their personal data in a commonly used machine-readable format, and transfer their personal data from one controller to another or have the data transmitted directly between controllers.
- **Right to withdraw consent**
  A data subject has the right to withdraw their consent at any time. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject must be informed of the right to withdraw consent. It must be as easy to withdraw consent as to give it.
- **Right to object to marketing**
  Data subjects have the right to object to the processing of personal data for the purpose of direct marketing, including profiling.
- **Right to complain to the relevant data protection authority(ies)**
  Data subjects have the right to lodge complaints concerning the processing of their personal data with the ICO, if the data subject lives in the UK or the alleged infringement occurred in the UK.
- **Right to basic information**
  Data subjects have the right to be provided with information on the identity of the controller, the reasons for processing their personal data and other relevant information necessary to ensure the fair and transparent processing of personal data.

## 6 Registration Formalities and Prior Approval

**6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?**

No, there is no longer a legal obligation on businesses to register with or notify the ICO as there was under the Data Protection Act 1998 (the "**DPA 1998**"). This requirement has been replaced by a legal obligation on controllers (not processors) to pay a data protection fee under the Data Protection (Charges and Information) Regulations 2018 (the "**2018 Regulations**") which came into force on 25 May 2018. As such, the following questions in this section will relate to the fee requirement instead of the registration requirement. It should be noted that certain businesses are exempt such as public authorities, charities and small occupational pension schemes.

In addition to the above, a controller must keep records of its processing activities which, upon request, must be disclosed to the ICO. Furthermore, a processor must keep records of its processing activities performed on behalf of a controller.

**6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?**

The information provided to the ICO need not be too detailed. Only the information listed in question 6.5 must be provided.

**6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?**

A separate fee is payable by every UK entity that acts as a controller.

**6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?**

Any controller that is subject to the DPA 2018 must pay the fee to the Information Commissioner unless it is exempt.

**6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?**

A controller must provide the ICO with the following information: contact details; number of staff; turnover for its financial year; type of organisation; and details of the Data Protection Officer (if applicable).

**6.6 What are the sanctions for failure to register/notify where required?**

The penalty for failing to pay the fee or paying the incorrect fee can be a maximum of 150% of the top-tier fee (see question 6.7 below).

**6.7 What is the fee per registration/notification (if applicable)?**

There are three tiers of fees ranging from £40 to £2,900 and the fee payable depends on the size of the business, its turnover and the type of business.

**6.8 How frequently must registrations/notifications be renewed (if applicable)?**

The fee is payable annually.

**6.9 Is any prior approval required from the data protection regulator?**

No, prior approval is not required.

**6.10 Can the registration/notification be completed online?**

Payment of the fee can be completed online through the ICO's website.

**6.11 Is there a publicly available list of completed registrations/notifications?**

Yes, there is a public register of controllers who pay the data protection fee.

**6.12 How long does a typical registration/notification process take?**

As payment can be completed online through the ICO website, this process can be immediate. Other payment methods (e.g., cheques) may be slower.

## 7 Appointment of a Data Protection Officer

**7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.**

The appointment of a Data Protection Officer for controllers or processors is only mandatory in some circumstances, including where there is: (i) large-scale regular and systematic monitoring of individuals; or (ii) large-scale processing of sensitive personal data.

Where a business designates a Data Protection Officer voluntarily, the requirements of the UK GDPR apply as though the appointment were mandatory.

**7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?**

In the circumstances where appointment of a Data Protection Officer is mandatory, failure to comply may result in the wide range of penalties available under the UK GDPR.

**7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?**

The appointed Data Protection Officer should not be dismissed or penalised for performing their tasks, and should report directly to the highest management level of the controller or processor.

**7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?**

A group of undertakings may appoint a single Data Protection Officer provided that the Data Protection Officer is easily accessible from each establishment.

**7.5 Please describe any specific qualifications for the Data Protection Officer required by law.**

The Data Protection Officer should be appointed on the basis of professional qualities and should have an expert knowledge of data protection law and practices. While this is not strictly defined, it is clear that the level of expertise required will depend on the circumstances. For example, the involvement of large volumes of sensitive personal data will require a higher level of knowledge.

**7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?**

A Data Protection Officer should be involved in all issues which relate to the protection of personal data. The UK GDPR outlines the minimum tasks required by the Data Protection Officer, which include: (i) informing the controller, processor and their relevant employees who process data of their obligations under the UK GDPR; (ii) monitoring compliance with the UK GDPR, other national data protection legislation and internal policies in relation to the processing of personal data including internal audits; (iii) advising on data protection impact assessments and the training of staff; and (iv) co-operating with the data protection authority and acting as the authority's primary contact point for issues related to data processing.

**7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?**

Yes, the controller or processor must notify the data protection authority of the contact details of the designated Data Protection Officer.

**7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?**

The Data Protection Officer does not necessarily need to be named in the public-facing privacy notice. However, the contact details of the Data Protection Officer must be notified to the data subject when personal data relating to that data subject are collected. As a matter of good practice, the Article 29 Working Party (the "**WP29**") (now the European Data Protection Board (the "**EDPB**")) recommended in its 2017 guidance on Data Protection Officers that both the data protection authority and employees should be notified of the name and contact details of the Data Protection Officer. This guidance is likely to remain persuasive despite the UK's departure from the EU.

## 8 Appointment of Processors

**8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?**

Yes. The business that appoints a processor to process personal data on its behalf is required to enter into an agreement with the processor which sets out the subject matter for processing, the duration of processing, the nature and purpose of processing, the types of personal data and categories of data subjects, and the obligations and rights of the controller (i.e., the business).

It is essential that the processor appointed by the business complies with the UK GDPR.

**8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?**

The processor must be appointed under a binding agreement in writing. The contractual terms must stipulate that the processor: (i) only acts on the documented instructions of the controller; (ii) imposes confidentiality obligations on all employees; (iii) ensures the security of personal data that it processes; (iv) abides by the rules regarding the appointment of sub-processors; (v) implements measures to assist the controller in guaranteeing the rights of data subjects; (vi) assists the controller in obtaining approval from the ICO; (vii) either returns or destroys the personal data at the end of the relationship (except as required by UK law); and (viii) provides the controller with all information necessary to demonstrate compliance with the UK GDPR.

## 9 Marketing

**9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).**

The PECR requires businesses to obtain consent before sending electronic communications to individuals for the purpose of direct marketing. There are exemptions to this; however, they are very narrow.

The European Commission is currently developing a new ePrivacy Regulation which, together with the GDPR, is likely to make it harder to engage in certain types of electronic direct marketing. The European Council agreed its position as to the revised draft ePrivacy Regulation on 10 February 2021. However, it is unclear when the Regulation will be finalised and implemented. Once implemented, it is possible that a similar harmonising regulation will be adopted in the UK.

**9.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?**

There are no specific restrictions applicable in a business-to-business context, although it is good practice for businesses to offer an opt-out of electronic direct marketing, such as emails or text messages, to other corporate bodies.

**9.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).**

The PECR does not prohibit all unsolicited marketing calls. However, the UK offers an opt-out register (the Telephone Preference Service (the "**TPS**")). It is a legal requirement not to make unsolicited marketing calls to numbers registered in the TPS, without the consent of the relevant individual subscriber.

**9.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?**

The PECR does not have formal extraterritoriality provisions and therefore cannot be applied where there is no nexus with the UK.

**9.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?**

Yes. The ICO has issued a number of fines to companies that breached direct marketing laws. Since 2018, there has been significant focus on "nuisance calls". In 2020, the fines for contacting individuals without their consent ranged from £40,000 to the maximum fine of £500,000. The maximum fine was issued to a company for making more than 193 million automated "nuisance calls". So far in 2021, the ICO has already issued a number of fines, including one fine of £250,000 to a company for sending more than 2.6 million nuisance text messages to customers without their valid consent.

**9.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?**

For a lawful purchase of a marketing list, the relevant individuals must have been originally informed by the seller that their data could be passed on to other businesses for marketing purposes and the individuals must have consented to that. The ICO recommends due diligence on any lists prior to purchase, and in practice, it is recommended that warranties are employed to ensure that the marketing list does not contravene these requirements.

**9.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?**

The maximum fine is £500,000, although typical fines are generally well below this level (with the exception of a few cases (e.g., see the answer to question 9.5 above) where the penalty imposed did in fact reach this maximum threshold).

## 10 Cookies

**10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).**

The PECR implements Article 5 of the ePrivacy Directive. Pursuant to Article 5 of the EU ePrivacy Directive, the storage of cookies (or other data) on an end user's device requires prior consent (the applicable standard of consent is derived from the GDPR). For consent to be valid, it must be informed, specific, freely given and must constitute a real and unambiguous indication of the individual's wishes (which has been interpreted by the Court of Justice of the European Union as requiring a "clear affirmative action"). This does not apply if: (i) the cookie is for the sole purpose of carrying out the transmission of a communication over an electronic communications network; or (ii) the cookie is strictly necessary to provide an "information society service" (e.g., a service over the internet) requested by the subscriber or user, which means that it must be essential to fulfil their request. The ICO stated in its Children's Code that cookies placed for the sole purpose of age verification are considered to be "essential", and therefore do not require consent.

The EU Commission intends to pass a new ePrivacy Regulation that will replace the respective national legislation in the EU Member States. The ePrivacy Regulation was planned to come into force in 2019. The European Council agreed its position as to the revised draft ePrivacy Regulation on 10 February 2021. It is, however, still a draft at this stage and it is unclear when it will be finalised. Once implemented, it is possible that a similar harmonising regulation will be adopted in the UK.

**10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?**

While it would not apply automatically in the UK, the draft ePrivacy Regulation envisages stricter consent requirements for the use of cookies. It would prevent businesses from accessing users' devices and collecting information unless: (i) it is necessary for the sole purpose of providing the service; (ii) they have the consent of the user prior to commencing tracking; (iii) cookies are used for the sole purpose of audience measuring (e.g., used to count the number of visitors to websites); (iv) necessary to maintain or restore security of the services provided, or of hardware, or to prevent fraud, or to prevent or detect technical faults; (v) necessary for a software update (subject to a number of requirements); or (vi) it is necessary to locate a device when an individual is making an emergency call. Under the PECR, no consent is required if the sole purpose of the cookie is carrying out the transmission of a communication or if it is strictly necessary to provide an information society service requested by the user.

**10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?**

The ICO has taken comparatively little enforcement action regarding cookies. However, it has released new cookies guidance which takes a noticeably stricter line. It remains to be seen how vigilantly this guidance will be enforced.

**10.4 What are the maximum penalties for breaches of applicable cookie restrictions?**

The maximum penalty is currently £500,000. The ICO has indicated that it will largely continue to follow its established procedure of information and enforcement notices, with fines issued only in the most serious cases. The maximum penalty will likely be increased to the higher of 4% of annual turnover or €20m under the ePrivacy Regulation, so as to align with penalties under the GDPR. It remains to be seen if the UK will take the same approach. If it does, the penalty will likely be the higher of 4% of annual turnover or £17.5m (so as to align with the UK GDPR).

## 11 Restrictions on International Data Transfers

**11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.**

Transfers of personal data to recipients outside of the UK can only take place if: (i) the transfer is to an "Adequate Jurisdiction" (as specified in the DPA 18 or as further specified by the ICO); or (ii) the transferor has implemented one of the required safeguards as specified by the UK GDPR; or (iii) one of the derogations specified in the UK GDPR applies to the relevant transfer. The EDPB Guidelines (2/2018) set out that a "layered approach" should be taken with respect to these transfer mechanisms. This guidance is likely to remain persuasive following the UK's departure from the EU. If the transfer is not to an Adequate Jurisdiction, the data exporter should first explore the possibility of implementing one of the safeguards provided for in the UK GDPR before relying on a derogation.

Following the Brexit Transition Period, the UK has become a third country for the purposes of EU law. The UK has sought an adequacy decision from the European Commission. If an adequacy decision is granted, it will be lawful to transfer personal data from the EEA to the UK without the need for additional protections. If an adequacy decision is not granted (or is granted but later revoked), then transfers of personal data from the EEA to the UK will be subject to the usual restrictions that apply under the GDPR with respect to transfers of personal data to any third country. In practice, this would typically mean that Standard Contractual Clauses ("SCCs") would need to be implemented between parties wishing to transfer data from the EEA to the UK.

On 28 December 2020, the UK and the EU agreed the Trade and Cooperation Agreement, which included provisions allowing transfers of personal data to continue temporarily until 1 July 2021, while the EU assessed whether the UK should receive an adequacy decision.

On 5 February 2021, the European Parliament's Committee on Civil Liberties, Justice and Home Affairs issued its own (non-binding) Opinion, which concluded that the UK should not

be granted an adequacy decision for several reasons, including perceived concerns around national security.

On 19 February 2021, the European Commission released its draft adequacy decisions, one in relation to the GDPR (which considers, among other things, the UK's general data protection framework and the level of access that the UK Government has to personal data for law enforcement and national security purposes) and one in relation to the LED (which assesses a number of topics including the UK's standards regarding police and judicial cooperation in criminal matters).

On 14 April 2021, the EDPB announced that it had adopted two Opinions on the draft UK adequacy decisions issued by the European Commission on 19 February 2021. The EDPB noted that there exist "key areas of strong alignment between the EU and the UK data protection frameworks". This reflects the fact that the UK's post-Brexit implementation of the UK GDPR is largely identical to the (EU) GDPR. In particular, the EDPB highlighted common ground on "grounds for lawful and fair processing for legitimate purposes; purpose limitation; data quality and proportionality; data retention, security and confidentiality; transparency; special categories of data; and on automated decision making and profiling".

If the decisions are adopted, the UK will join the short list of non-EEA countries to which EEA personal data may flow without restriction. Currently this list includes Andorra, Argentina, Canada (commercial organisations), the Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay. South Korea is also expected to be granted adequate status soon.

Now that the EDPB has provided its Opinions, the European Commission will seek approval from representatives from each EU Member State. Once that process is completed, the European Commission will adopt a final decision regarding the adequacy decisions.

If adopted, the adequacy decisions would be valid for a period of four years, after which the adequacy decisions may be renewed if the UK's data protection regime continues to be deemed adequate. However, adequacy decisions can be revoked. See the example discussion question 11.2.

**11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).**

When transferring personal data to a country other than an Adequate Jurisdiction, businesses must ensure that there are appropriate safeguards on the data transfer, as prescribed by the UK GDPR. The UK GDPR offers a number of ways to ensure compliance for international data transfers, of which one is consent of the relevant data subject. Other common options are the use of SCCs or Binding Corporate Rules ("**BCRs**").

The EU Commission maintains two sets of SCCs – these are available for transfers between controllers, and transfers between a controller (as exporter) and a processor (as importer). The ICO has published UK versions of the SCCs, with suggested changes to reflect the fact that the UK is no longer a member of the EU. Businesses may choose to adopt these new UK SCCs, or may choose to continue to rely upon the existing EU Commission-approved SCCs. International data transfers may also take place on the basis of contracts agreed between the data exporter and data importer provided that they conform to the protections outlined in the UK GDPR, and they have prior approval by the ICO.

International data transfers within a group of businesses can be safeguarded by the implementation of BCRs. The BCRs will always need approval from the ICO. Most importantly, the BCRs will need to include a mechanism to ensure they are legally binding and enforced by every member in the group of businesses. Among other things, the BCRs must set out the group structure of the businesses, the proposed data transfers and their purpose, the rights of data subjects, the mechanisms that will be implemented to ensure compliance with the UK GDPR and the relevant complainant procedures.

Following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18), transfers of personal data to the USA on the basis of the EU-US Privacy Shield Framework are no longer valid.

**11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.**

It is likely that the international transfer of data will require prior approval from the ICO unless they have already established a UK GDPR-compliant mechanism, as set out above, for such transfers.

In any case, most of the safeguards outlined in the UK GDPR will need initial approval from the data protection authority, such as the establishment of BCRs.

**11.4 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?**

The EDPB has issued draft Recommendations 01/2020 on supplementary protections to be implemented where appropriate, in respect of transfers made under SCCs, in light of the *Schrems II* decision.

In *Schrems II*, the court held that organisations could continue to rely upon SCCs to transfer EU personal data to third countries, so long as "supplementary measures" are established in order to ensure adequate levels of protection for transferred personal data.

The EDPB's Recommendations set out what these "supplementary measures" could be in practice. These include technical, contractual and organisational measures.

While the ICO is no longer bound to follow the guidance of the EDPB, its recommendations are likely to remain persuasive in the UK.

**11.5 What guidance (if any) has/have the data protection authority(ies) issued in relation to the European Commission's revised Standard Contractual Clauses?**

The ICO has published UK versions of the SCCs, with suggested changes to reflect the fact that the UK is no longer a member of the EU, along with associated guidance. The ICO has also declared its intention to consult on and publish new UK SCCs during 2021. With respect to the European Commission's revised SCCs, these will not apply automatically in the UK. However,

the EDPB and the European Data Protection Supervisor have issued Joint Opinion 1/2021 in relation to the [draft] revised SCCs. These opinions are likely to remain persuasive to the ICO as it develops new UK SCCs.

## 12 Whistle-blower Hotlines

**12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?**

Internal whistle-blowing schemes are generally established in pursuance of a concern to implement proper corporate governance principles in the daily functioning of businesses. Whistle-blowing is designed as an additional mechanism for employees to report misconduct internally through a specific channel and supplements a business' regular information and reporting channels, such as employee representatives, line management, quality-control personnel or internal auditors who are employed precisely to report such misconduct.

The WP29 has limited its Opinion 1/2006 on the application of EU data protection rules to internal whistle-blowing schemes to the fields of accounting, internal accounting controls, auditing matters, the fight against bribery, banking and financial crime. The scope of corporate whistle-blower hotlines, however, does not need to be limited to any particular issues. In the Opinion, it is recommended that the business responsible for the whistle-blowing scheme should carefully assess whether it might be appropriate to limit the number of persons eligible for reporting alleged misconduct through the whistle-blowing scheme, and whether it might be appropriate to limit the number of persons who may be reported through the scheme; in particular, in the light of the seriousness of the alleged offences reported. This guidance likely remains persuasive following the UK's departure from the EU.

**12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?**

Anonymous reporting is not prohibited under UK data protection law; however, it raises problems as regards the essential requirement that personal data should only be collected fairly. In Opinion 1/2006, the WP29 considered that only identified reports should be advertised in order to satisfy this requirement. This guidance likely remains persuasive following the UK's departure from the EU. Businesses should not encourage or advertise the fact that anonymous reports may be made through a whistle-blower scheme.

An individual who intends to report to a whistle-blowing system should be aware that he/she will not suffer due to his/her action. The whistle-blower, at the time of establishing the first contact with the scheme, should be informed that his/her identity will be kept confidential at all the stages of the process, and in particular will not be disclosed to third parties, such as the incriminated person or the employee's line management. If, despite this information, the person reporting to the scheme still wants to remain anonymous, the report will be accepted into the scheme. Whistle-blowers should be informed that their identity may need to be disclosed to the relevant people involved in any further investigation or subsequent judicial proceedings instigated as a result of any enquiry conducted by the whistle-blowing scheme.

## 13 CCTV

**13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?**

A data protection impact assessment ("**DPIA**") must be undertaken with assistance from the Data Protection Officer when there is systematic monitoring of a publicly accessible area on a large scale. If the DPIA suggests that the processing would result in a high risk to the rights and freedoms of individuals prior to any action being taken by the controller, the controller must consult the ICO.

During the course of a consultation, the controller must provide information on the responsibilities of the controller and/or processors involved, the purpose of the intended processing, a copy of the DPIA, the safeguards provided by the UK GDPR to protect the rights and freedoms of data subjects and, where applicable, the contact details of the Data Protection Officer.

If the ICO is of the opinion that the CCTV monitoring would infringe the UK GDPR, it has to provide written advice to the controller within eight weeks of the request of a consultation and can use any of its wider investigative, advisory and corrective powers outlined in the UK GDPR.

**13.2 Are there limits on the purposes for which CCTV data may be used?**

Personal data must be collected only for specified and legitimate purposes and must be used only in a manner which is not incompatible with the original purpose. For example, if a CCTV camera is used for the purpose of monitoring criminal activity in an office, it cannot later be used for a new and fundamentally different purpose (e.g., monitoring the work attendance of employees) without the provision of fresh notice to the affected individuals and, where appropriate, the obtaining of consent in advance.

## 14 Employee Monitoring

**14.1 What types of employee monitoring are permitted (if any), and in what circumstances?**

Employee monitoring must be lawful and fair. Employers must consider whether the monitoring methods are too intrusive, such that the employer's legitimate interest is outweighed by the right to privacy. Employees must be notified of the extent of the monitoring prior to commencement, and why it is taking place.

**14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.**

The UK GDPR requires a lawful basis for the monitoring of employees (e.g., consent or legitimate interests). However, consent is rarely used as it could easily be withheld or withdrawn by employees. In addition, because of the imbalance of power in the relationship between employer and employee, consent given in an employment context is unlikely to be deemed "freely given", and therefore would not be valid. Generally, employers rely on the lawful basis of legitimate interests. This is subject to an assessment of proportionality and necessity. Employees must be given notice of the monitoring activities.

**14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?**

As good practice, trade unions and employee representatives should be consulted where applicable.

## 15 Data Security and Data Breach

**15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?**

Yes. Personal data must be processed in a way which ensures security and safeguards against unauthorised or unlawful processing, accidental loss, destruction and damage of the data.

Both controllers and processors must ensure they have appropriate technical and organisational measures to meet the requirements of the UK GDPR. Depending on the security risk, this may include the encryption of personal data, the ability to ensure the ongoing confidentiality, integrity and resilience of processing systems, an ability to restore access to data following a technical or physical incident, and a process for regularly testing and evaluating the technical and organisational measures for ensuring the security of processing.

**15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

The controller is responsible for reporting a personal data breach without undue delay (and in any case within 72 hours of first becoming aware of the breach) to the ICO, unless the breach is unlikely to result in a risk to the rights and freedoms of the data subject(s). A processor must notify any data breach to the controller without undue delay.

The notification must include the nature of the personal data breach, including the categories and number of data subjects concerned, the name and contact details of the Data Protection Officer or relevant point of contact, the likely consequences of the breach and the measures taken to address the breach, including attempts to mitigate possible adverse effects.

**15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

Controllers have a legal requirement to communicate the breach to the data subject, without undue delay, if the breach is likely to result in a high risk to the rights and freedoms of the data subject.

The notification must include the name and contact details of the Data Protection Officer (or point of contact), the likely consequences of the breach and any measures taken to remedy or mitigate the breach.

The controller may be exempt from notifying the data subject if the risk of harm is remote (e.g., because the affected data is encrypted), the controller has taken measures to minimise the risk of harm (e.g., suspending affected accounts) or the notification requires a disproportionate effort (e.g., a public notice of the breach).

**15.4 What are the maximum penalties for data security breaches?**

The maximum penalty is the higher of £17.5 million or 4% of worldwide turnover.

## 16 Enforcement and Sanctions

**16.1 Describe the enforcement powers of the data protection authority(ies).**

(a) **Investigative Powers**: The ICO has wide powers to order the controller and the processor to provide any information it requires for the performance of its tasks, to conduct investigations in the form of data protection audits, to carry out reviews on certificates issued pursuant to the UK GDPR, to notify the controller or processor of alleged infringements of the UK GDPR, to access all personal data and all information necessary for the performance of controllers' or processors' tasks and to access the premises of the data including any data processing equipment.

(b) **Corrective Powers**: The ICO has a wide range of powers including the ability to issue warnings or reprimands for non-compliance, to order the controller to disclose a personal data breach to the data subject, to impose a permanent or temporary ban on processing, to withdraw a certification and to impose an administrative fine (as below).

(c) **Authorisation and Advisory Powers**: The ICO has a wide range of powers to advise the controller, accredit certification bodies and to authorise certificates, contractual clauses, administrative arrangements and BCRs as outlined in the UK GDPR.

(d) **Imposition of administrative fines for infringements of specified GDPR provisions**: The UK GDPR provides for administrative fines of up to the greater of £17.5 million or 4% of the business' worldwide annual turnover during the preceding financial year.

(e) **Non-compliance with a data protection authority**: The UK GDPR provides for administrative fines of up to the greater of £17.5 million or 4% of the business' worldwide annual turnover during the preceding financial year.

**16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?**

The UK GDPR entitles the ICO to impose a temporary or definitive limitation, including a ban on processing.

**16.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.**

The ICO tends to co-operate with businesses before it takes enforcement action.

**16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?**

The UK GDPR can also apply to non-UK businesses even if

they have no physical presence in the UK (see the answer to question 3.1 above). Such businesses must appoint a representative in the UK against which the ICO can take relevant enforcement action under the UK GDPR.

## 17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

### 17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Most businesses will weigh the risks presented by non-compliance with the relevant foreign court order against those of non-compliance with the DPA 2018 and determine which are lower. Assuming that the business decides to disclose the requested personal data, businesses will usually seek to justify such disclosures on the basis that they are necessary for the establishment, exercise or defence of legal claims.

### 17.2 What guidance has/have the data protection authority(ies) issued?

There is currently no standalone guidance from the ICO on this point under the DPA 2018.

## 18 Trends and Developments

### 18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

In the last 12 months, the ICO has issued substantial fines under the GDPR. For example, in October 2020, the ICO issued a penalty notice to impose a fine of £20 million on British Airways for allegedly failing to adequately safeguard customers' personal data, resulting in the personal data of 500,000 customers being compromised. This is a significant reduction from the £183 million the ICO had previously proposed.

### 18.2 What "hot topics" are currently a focus for the data protection regulator?

The largest single hot topic for the ICO at present is the impact of Brexit on transfers of personal data between the EU and the UK. Following the end of the Brexit Transition Period, the UK is a third country for the purposes of EU law. The UK has sought an adequacy decision from the European Commission. If an adequacy decision is granted, it will be lawful to transfer personal data from the EEA to the UK without the need for additional protections. If an adequacy decision is not granted, then transfers of personal data from the EEA to the UK will be subject to the restrictions that apply under the GDPR with respect to transfers of personal data to any third country. In practice, this would typically mean that SCCs would need to be implemented between parties wishing to transfer data from the EEA to the UK.

Please see question 11.1 for further information on this topic.

**Tim Hickman** is a partner in the London office of White & Case, is dual-qualified in England & Wales and the Republic of Ireland, and advises on all aspects of UK and EU privacy and data protection law. Tim has significant experience of working with a wide range of clients in the EU, Asia and the US.

He has spent time on secondment at Google, advising on cutting-edge privacy and data protection issues. He has also spoken at several events at Harvard Law School, and he delivered the closing address at the Harvard European Law Conference 2019.

"Tim Hickman's knowledge of data protection law is second to none. He is also personable and easy to work with ... Clients appreciate the examples he provides, making the advice more tangible." – *The Legal 500 2020*.

**White & Case LLP**
5 Old Broad Street
London, EC2N 1DW
United Kingdom

Tel: +44 7532 2517
Email: tim.hickman@whitecase.com
URL: www.whitecase.com

**Joe Devine** is an associate in the London office of White & Case, is qualified in England & Wales, has a detailed knowledge of the EU's General Data Protection Regulation (GDPR) and the UK's Data Protection Act 2018, and regularly advises clients on all aspects of privacy and data protection law compliance.

**White & Case LLP**
5 Old Broad Street
London, EC2N 1DW
United Kingdom

Tel: +44 20 7532 1206
Email: joe.devine@whitecase.com
URL: www.whitecase.com

With one of the largest and most experienced data privacy and cybersecurity groups in the world, White & Case's global team is on hand to guide clients through the relevant data protection legislation in the jurisdictions in which they are active. Seamlessly working with their counterparts in other practice areas, our global team has the depth of resources to provide integrated, creative and practical advice on the privacy-related concerns faced by our clients, wherever they are located.

Our experience spans the full range of industry sectors including financial institutions and banking, biotechnology, pharmaceuticals and chemicals, construction and engineering, consumer goods and retail, automotive, hotels and leisure, IT, telecommunications, internet and social media, manufacturing and electronics, publishing and media.

**www.whitecase.com**

# USA


F. Paul Pittman


Kyle Levenberg

White & Case LLP

## 1 Relevant Legislation and Competent Authorities

### 1.1 What is the principal data protection legislation?

There is no single principal data protection legislation in the United States (U.S.). Rather, a jumble of hundreds of laws enacted on both the federal and state levels serve to protect the personal data of U.S. residents. At the federal level, the Federal Trade Commission Act (15 U.S. Code § 41 *et seq.*) broadly empowers the U.S. Federal Trade Commission (FTC) to bring enforcement actions to protect consumers against unfair or deceptive practices and to enforce federal privacy and data protection regulations. The FTC has taken the position that "deceptive practices" include a company's failure to comply with its published privacy promises and its failure to provide adequate security of personal information, in addition to its use of deceptive advertising or marketing methods.

As described more fully below, other federal statutes primarily address specific sectors, such as financial services or healthcare. In parallel to the federal regime, state-level statutes protect a wide range of privacy rights of individual residents. The protections afforded by state statutes often differ considerably from one state to another, and some are comprehensive, while others cover areas as diverse as protecting library records to keeping homeowners free from drone surveillance.

### 1.2 Is there any other general legislation that impacts data protection?

Although there is no general federal legislation impacting data protection, there are a number of federal data protection laws that are sector-specific (see question 1.3 below), or focus on particular types of data. By way of example, the Driver's Privacy Protection Act of 1994 (DPPA) (18 U.S. Code § 2721 *et seq.*) governs the privacy and disclosure of personal information gathered by state Departments of Motor Vehicles. Child information is protected at the federal level under the Children's Online Privacy Protection Act (COPPA) (15 U.S. Code § 6501), which prohibits the collection of any information from a child under the age of 13 online and from digitally connected devices, and requires publication of privacy notices and collection of verifiable parental consent when information from children is being collected. The Video Privacy Protection Act (VPPA) (18 U.S. Code § 2710 *et seq.*) restricts the disclosure of rental or sale records of videos or similar audio-visual materials, including online streaming. Similarly, the Cable Communications Policy Act of 1984 includes provisions dedicated to the protection of subscriber privacy (47 U.S. Code § 551).

State laws also may impose restrictions and obligations on businesses relating to the collection, use, disclosure, security, or retention of special categories of information, such as biometric data, medical records, SSNs, driver's licence information, email addresses, library records, television viewing habits, financial records, tax records, insurance information, criminal justice information, phone records, and education records, just to name some of the most common.

Every state has adopted data breach notification legislation that applies to certain types of personal information about its residents. Even if a business does not have a physical presence in a particular state, it typically must comply with the state's laws when faced with the unauthorised access to, or acquisition of, personal information it collects, holds, transfers or processes about that state's residents. The types of information subject to these laws vary, with most states defining personal information to include an individual's first name or first initial and last name, together with a data point including the individual's SSN, driver's licence or state identification card number, financial account number or payment card information.

Some states are more active than others when it comes to data protection. Massachusetts, for example, has strong data protection regulations (201 CMR 17.00), requiring any entity that receives, stores, maintains, processes, or otherwise has access to "personal information" of a Massachusetts resident in connection with the provision of goods or services, or in connection with employment, (a) to implement and maintain a comprehensive written information security plan (WISP) addressing 10 core standards, and (b) to establish and maintain a formal information security programme that satisfies eight core requirements, which range from encryption to information security training.

In 2019, New York expanded its data breach notification law to include the express requirement that entities develop, implement and maintain "reasonable" safeguards to protect the security, confidentiality and integrity of private information. Significantly, New York's SHIELD Act (N.Y. Gen Bus. Law § 899-bb) identifies a series of administrative, technical, and physical safeguards which, if implemented, are deemed to satisfy New York's reasonableness standard under the law. Previously, New York prioritised the regulation of certain financial institutions doing business in the state, by setting minimum cybersecurity standards, with requirements for companies to perform periodic risk assessments and file annual compliance certifications (23 NYCRR 500).

Illinois has a uniquely expansive state law (740 ILCS 14/), which imposes requirements on businesses that collect or otherwise obtain biometric information. The Illinois Biometric

Information Privacy Act (BIPA) is notable as, at the time of writing, it is the only state law regulating biometric data usage that allows private individuals to sue and recover damages for violations. In January 2019, the Illinois Supreme Court offered an expansive reading of the protections of the BIPA, holding that the law does not require individuals to show they suffered harm other than a violation of their legal rights to sue.

California has a long history of adopting privacy-forward legislation, and in 2018, the state enacted the California Consumer Privacy Act (CCPA), which became effective on January 1, 2020. The law introduced new obligations on covered businesses, including requirements to disclose the categories of personal information the business collects about consumers, the specific pieces of personal information the business collected about the consumer, the categories of sources from which the personal information is collected, the business or commercial purpose for collecting or selling personal information, and the categories of third parties with which the business shares personal information. It also introduced new rights for California residents, including the right to request access to and deletion of personal information and the right to opt out of having personal information sold to third parties.

More recently, we have seen a number of states push towards enacting comprehensive consumer data privacy laws. Specifically, in 2020, California amended the CCPA with the California Privacy Rights Act (CPRA) which expanded the rights granted to consumers and increased compliance obligation on businesses. In addition, in early 2021 Virginia enacted the Consumer Data Protection Act (CDPA) becoming the second state with a comprehensive data privacy law. These recently passed laws will come into effect on January 1, 2023, but may represent an opening of the floodgates in data privacy law at the state level. At the time of writing, the authors are aware of 20 comprehensive privacy bills before the legislatures of 15 different states.

### 1.3 Is there any sector-specific legislation that impacts data protection?

Key sector-specific laws include those covering financial services, healthcare, telecommunications, and education.

The Gramm Leach Bliley Act (GLBA) (15 U.S. Code § 6802(a) *et seq.*) governs the protection of personal information in the hands of banks, insurance companies and other companies in the financial service industry. This statute addresses "Non-Public Personal Information" (NPI), which includes any information that a financial service company collects from its customers in connection with the provision of its services. It imposes requirements on financial service industry companies for securing NPI, restricting disclosure and use of NPI and notifying customers when NPI is improperly exposed to unauthorised persons.

The Fair Credit Reporting Act (FCRA), as amended by the Fair and Accurate Credit Transactions Act (FACTA) (15 U.S. Code § 1681), restricts use of information with a bearing on an individual's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living to determine eligibility for credit, employment or insurance. It also requires the truncation of credit card numbers on printed receipts, requires the secure destruction of certain types of personal information, and regulates the use of certain types of information received from affiliated companies for marketing purposes.

In addition to financial industry laws and regulation, the major credit card companies require businesses that process, store or transmit payment card data to comply with the Payment Card Industry Data Security Standard (PCI-DSS).

The Health Information Portability and Accountability Act, as amended (HIPAA) (29 U.S. Code § 1181 *et seq.*) protects information held by a covered entity that concerns health status, provision of healthcare or payment for healthcare that can be linked to an individual. Its Privacy Rule regulates the collection and disclosure of such information. Its Security Rule imposes requirements for securing this data.

The Telephone Consumer Protection Act (TCPA) (47 U.S. Code § 227) and associated regulations regulate calls and text messages to mobile phones, and regulate calls to residential phones that are made for marketing purposes or using automated dialling systems or pre-recorded messages.

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g) provides students with the right to inspect and revise their student records for accuracy, while also prohibiting the disclosure of these records or other personal information on the student, without the student's or parent's (in some instances) consent.

Where a federal statute covers a specific topic, the federal law may pre-empt any similar state law on that topic. However, certain federal laws, like the GLBA for instance, specify that they are not pre-emptive of state laws on the subject.

### 1.4 What authority(ies) are responsible for data protection?

While the United States has no plenary data protection regulator at the federal level, the FTC's authority is very broad, and often sets the tone on federal privacy and data security issues. In addition, a variety of other agencies regulate data protection through sectoral laws, including the Office of the Comptroller of the Currency (OCC), the Department of Health and Human Services (HHS), the Federal Communications Commission (FCC), the Securities and Exchange Commission, the Consumer Financial Protection Bureau (CFPB) and the Department of Commerce. At the state level, the recently enacted CPRA created the first agency focused on data protection in the U.S., the California Privacy Protection Agency (CPPA).

## 2 Definitions

### 2.1 Please provide the key definitions used in the relevant legislation:

- "**Personal Data**"
  In the United States, information relating to an individual is typically referred to as "personal information" (rather than personal data). The definition of personal information in the U.S. is not uniform across all states or all regulations. In addition, certain data may be considered personal information for one purpose but not for another.
- "**Processing**"
  This is not applicable in our jurisdiction.
- "**Controller**"
  This is not applicable in our jurisdiction.
- "**Processor**"
  This is not applicable in our jurisdiction.
- "**Data Subject**"
  The state data protection statutes typically cover a "consumer" residing within the state. The definition of "consumer" differs by state. Under many state data protection statutes, a "consumer" is an individual who engages with a business for personal, family or household purposes. In contrast, under the California Consumer Privacy Act (CCPA) a "consumer" is defined broadly as a "natural person who is a California resident".
- "**Sensitive Personal Data**"
  This is not applicable in our jurisdiction.

- "**Data Breach**"
  The definition of a Data Breach depends on the individual state statute, but typically involves the unauthorised access or acquisition of computerised data that compromises the security, confidentiality, or integrity of personal information.

## 3 Territorial Scope

**3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?**

Businesses established in other jurisdictions may be subject to both federal and state data protection laws for activities impacting United States residents whose information the business collects, holds, transmits, processes or shares.

## 4 Key Principles

**4.1 What are the key principles that apply to the processing of personal data?**

- **Transparency**
  The FTC has issued guidelines espousing the principle of transparency, recommending that businesses: (i) provide clearer, shorter, and more standardised privacy notices that enable consumers to better comprehend privacy practices; (ii) provide reasonable access to the consumer data they maintain that is proportionate to the sensitivity of the data and the nature of its use; and (iii) expand efforts to educate consumers about commercial data privacy practices.
- **Lawful basis for processing**
  While there is no "lawful basis for processing" requirement under U.S. law, the FTC recommends that businesses provide notice to consumers of their data collection, use and sharing practices and obtain consent in limited circumstances where the use of consumer data is materially different than claimed when the data was collected, or where sensitive data is collected for certain purposes.
- **Purpose limitation**
  The FTC recommends privacy-by-design practices that include limiting "data collection to that which is consistent with the context of a particular transaction or the consumer's relationship with the business, or as required or specifically authorized by law".
- **Data minimisation**
  See above.
- **Proportionality**
  See above.
- **Retention**
  The FTC recommends privacy-by-design practices that implement "reasonable restrictions on the retention of data", including disposal "once the data has outlived the legitimate purpose for which it was collected".

## 5 Individual Rights

**5.1 What are the key rights that individuals have in relation to the processing of their personal data?**

- **Right of access to data/copies of data**
  These rights are statute-specific. For example, under certain circumstances, employees are entitled to receive copies of data held by employers. In other circumstances, parents are entitled to receive copies of information collected online from their children under the age of 13. Under HIPAA, individuals are entitled to request copies of medical information held by a health services provider. Further, the CCPA provides a right of access for California residents to personal information held by a business relating to that resident.
- **Right to rectification of errors**
  These rights are statute-specific. Some laws, such as the FCRA, provide consumers with a right to review data about the consumer held by an entity and request corrections to errors in that data. At the state level, the right to correct information commonly attaches to credit reports, as well as criminal justice information, employment records, and medical records.
- **Right to deletion**
  These rights are statute-specific. By way of federal law example, COPPA provides parents the right to review and delete their children's information and may require that data be deleted even in the absence of a request. Some state laws, such as the CCPA and the CDPA, provide a right of deletion for residents of the respective states, with certain exceptions.
- **Right to object to processing**
  These rights are statute-specific. Individuals are given the right to opt out of receiving commercial (advertising) emails under CAN-SPAM and the right to not receive certain types of calls to residential or mobile telephone numbers without express consent under the TCPA. Some states provide individuals with the right not to have telephone calls recorded without either consent of all parties to the call or consent of one party to the call.
- **Right to restrict processing**
  These rights are statute-specific. Certain laws restrict how an entity may process consumer data. For example, the CCPA allows California residents, and the Nevada Privacy Law allows Nevada residents to prohibit a business from selling that individual's personal information. The newly enacted CDPA will provide a right to restrict processing for the purposes of sale, targeted advertising, and profiling.
- **Right to data portability**
  These rights are statute-specific. Examples of consumer rights to data portability exist under HIPAA, where individuals are entitled to request that medical information held by a health services provider be transferred to another health services provider. In addition, the CCPA provides a right of data portability for California residents.
- **Right to withdraw consent**
  These rights are statute-specific. By way of example, under the TCPA, individuals are permitted to withdraw consent given to receive certain types of calls or texts to residential or mobile telephone lines.
- **Right to object to marketing**
  These rights are statute-specific. Several laws permit consumers to restrict marketing activities involving their personal data. Under CAN-SPAM, for example, individuals may opt out of receiving commercial (advertising) emails. Under the TCPA, individuals must provide express written consent to receive marketing calls/texts to mobile telephone lines. California's Shine the Light Act requires companies that share personal information for the recipient's direct marketing purposes to either provide an opt-out or make certain disclosures to the consumer of what information is shared, and with whom.
- **Right to complain to the relevant data protection authority(ies)**
  These rights are statute-specific. By way of example,

individuals may report unwanted or deceptive commercial email ("spam") directly to the FTC, and telemarketing violations directly to the FCC. Similarly, anyone may file a HIPAA complaint directly with the Department of Health and Human Services (HHS). At the state level, California residents may report alleged violations of the CCPA to the California Attorney General.

## 6 Registration Formalities and Prior Approval

**6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?**

Both Vermont and California require data brokers to register with the state attorney general. The Vermont requirement, which went into effect in 2019, defines a "data broker" to include entities that knowingly collect and sell or license to third parties the personal information of a consumer with whom the business does not have a direct relationship (9 V.S.A. chapter 62). California's requirement went into effect in 2020, and similarly applies to the knowing collection and sale of personal information regarding consumers with which the business does not have a direct relationship (Cal. Civ. Code § 1798.99.82).

**6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?**

The states that have mandated data broker registration generally do not require a specific description of relevant data processing activities. California makes it optional for the data broker to provide within its registration any information concerning its data collection practices (Cal. Civ. Code § 1798.99.82). Vermont, in contrast, is more demanding and requires registrants to disclose information regarding consumer opt-out, whether the data broker implements a purchaser credentialing process, and the number and extent of any data broker security breaches it experienced during the prior year. Where data brokers knowingly possess information about minors, Vermont law requires that they detail all related data collection practices, databases, sales activities, and opt-out policies (9 V.S.A. § 2446).

**6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?**

Data broker registrations are made on a "per legal entity" basis.

**6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?**

Within the states for which it applies, registrations are required based on the business falling within the definition of a "data broker" pursuant to state law. Generally, a "data broker" is defined as a business that knowingly collects and sells the personal information of a consumer with whom the business does not have a direct relationship.

**6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?**

See question 6.2 above.

**6.6 What are the sanctions for failure to register/notify where required?**

In Vermont, the penalty is US$150 per day in addition to the registration fee of US$100. In California, a data broker that fails to register is liable for civil penalties, fees, and costs of US$100 for each day the data broker fails to register and an amount equal to the fees that were due during the period it failed to register.

**6.7 What is the fee per registration/notification (if applicable)?**

Fees vary by state. The data broker registration fee in Vermont is US$100 and in California it is US$360.

**6.8 How frequently must registrations/notifications be renewed (if applicable)?**

In both Vermont and California, data brokers are required to register annually.

**6.9 Is any prior approval required from the data protection regulator?**

Data broker registration submissions require Attorney General approval in both Vermont and California.

**6.10 Can the registration/notification be completed online?**

Data broker registration for both Vermont and California may be completed online.

**6.11 Is there a publicly available list of completed registrations/notifications?**

Vermont and California maintain publicly available lists of registered data brokers.

**6.12 How long does a typical registration/notification process take?**

Neither Vermont nor California publish information concerning the typical amount of time for the data broker registration process.

## 7 Appointment of a Data Protection Officer

**7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.**

Appointment of a Data Protection Officer is not required under U.S. law, but certain statutes require the appointment or designation of an individual or individuals who are charged with compliance with the privacy and data security requirements under the statute. These include the GLBA, HIPAA, and the Massachusetts Data Security Regulation, for example.

**7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?**

Potential sanctions are statute/regulator-specific.

**7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?**

This is not applicable in our jurisdiction.

**7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?**

This is not applicable in our jurisdiction.

**7.5 Please describe any specific qualifications for the Data Protection Officer required by law.**

This is not applicable in our jurisdiction.

**7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?**

This is not applicable in our jurisdiction.

**7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?**

This is not applicable in our jurisdiction.

**7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?**

This is not applicable in our jurisdiction.

## 8 Appointment of Processors

**8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?**

Under certain state laws and federal regulatory guidance, if a business shares certain categories of personal information with a vendor, the business is required to contractually bind the vendor to reasonable security practices. HIPAA, for example, requires the use of Business Associate Agreements for the transfer of protected health information to vendors. Another example is the CCPA, which requires written contracts with service providers.

**8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?**

The form of the contract typically is not specified. HIPAA, however, is an example of a statute with minimum requirements for provisions that must be included within Business Associate Agreements. These agreements must include limitations on use and disclosure, and require vendors to abide by HIPAA's Security Rule, to provide breach notification and report on unauthorised use and disclosure, to return or destroy protected data, and to make its books, records, and practices available to the federal regulator. Under the CCPA, the contract must restrict the service provider from retaining, using, or disclosing personal information for any purpose other than performance of the services specified in the contract.

## 9 Marketing

**9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).**

Prior express written consent is required under the TCPA before certain marketing texts may be sent to a mobile telephone line. Other federal statutes have opt-out rather than opt-in consent requirements. For instance, under CAN-SPAM, marketing emails – or emails sent for the primary purpose of advertising or promoting a commercial product or service – may be sent to those not opting out, provided the sender is accurately identified, the subject line and text of the email are not deceptive, the email contains the name and address of the sender, the email contains a free, simple mechanism to opt out of future emails, and the sender honours opt-outs within 10 days of receipt.

**9.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?**

The TCPA and CAN-SPAM Act apply to both business-to-consumer and business-to-business electronic direct marketing. In contrast, business-to-business telephone communications, except those intended to induce the retail sale of non-durable office or cleaning supplies, are exempt from the Telemarketing Sales Rule described in question 9.3 below.

**9.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).**

Marketing by telephone is regulated on the national level by the Telemarketing Sales Rule, a regulation under the Telemarketing

and Consumer Fraud and Abuse Prevention Act. This act established the national Do Not Call list of telephone numbers that cannot be used for marketing communications (calls and texts) and disclosure requirements for companies engaging in telephone marketing. It also proscribes limitations on the use of telephone marketing, including, for instance, limiting the time of day for marketing calls, requiring the caller to provide an opt-out of future calls, and limiting the use of pre-recorded messages. There are no consent or opt-out requirements for sending marketing materials through postal mail. In addition, with the growing prevalence of telemarketers using fake caller IDs, the FCC is becoming more aggressive with its enforcement of the Truth in the Caller ID Act.

It is noted that the FTC, which regulates deceptive practices, has brought enforcement actions relating to the transmission of marketing emails or telemarketing calls by companies who have made promises in their publicly posted privacy policies that personal information will not be used for marketing purposes. Additionally, many states apply deceptive practices statutes to impose penalties or injunctive relief in similar circumstances, or where violation of a federal statute is deemed a deceptive practice under state law. Finally, comprehensive state data privacy laws in California and Virginia offer consumers an opt-out of sale, disclosure, or processing of personal information in relation to targeted advertising or profiling. Although we are yet to see the impact of these provisions on the advertising ecosystem, this will likely prove to be a space to watch over the coming years.

**9.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?**

Yes, if the recipient is within the United States.

**9.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?**

The FTC, FCC, and the Attorneys General of the states are active in enforcement in this area.

**9.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?**

Yes; however, the purchaser of the list should "scrub" it against the national Do Not Call list and the purchaser's email opt-out lists. Some states forbid the sale of email addresses of individuals who have opted out of receiving marketing emails, and some forbid the sale of information obtained in connection with a consumer's purchase transaction.

**9.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?**

The penalties under CAN-SPAM can range from US$16,000 to US$43,792 per email. The penalties under the TCPA are US$500 per telephone call/text message violation, US$1,500 for each wilful or knowing violation, and additional civil forfeiture fees of up to US$10,000 for intentional violations (based on the TRACED Act, passed in 2019), plus fines that can reach US$16,000 for each political message or call sent in violation of the Act. By way of example, the FTC and the attorneys general of several states obtained a judgment of US$280 million in 2017 for a company's repeated violation (involving over 66 million calls) of the TCPA, the FTC's Telemarketing Sales Rule, and state law. Similarly, in March 2021, the FCC issued a US$225 million fine – the largest in the history of the agency – against telemarketers based in Texas for violations of the TCPA and the Truth in Caller ID Act in connection with approximately 1 billion robocalls.

Many states have their own deceptive practices statutes, which impose additional state penalties where violations of federal statutes are deemed to be deceptive practices under the state statute.

## 10 Cookies

**10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).**

The federal Computer Fraud and Abuse Act has been used to assert legal claims against the use of cookies for behavioural advertising, where the cookies enable "deep packet" inspection of the computer on which they are placed. At least two states, California and Delaware, require disclosures to be made where cookies are used to collect information about a consumer's online activities across different websites or over time. The required disclosure must include how the operator responds to so-called "do not track" signals or other similar mechanisms.

In addition, the FTC Act and state deceptive practices acts have underpinned regulatory enforcement and private class action lawsuits against companies that failed to disclose or misrepresented their use of tracking cookies. One company settled an action in 2012 with a payment of US$22.5 million to the FTC, and in 2016 agreed to pay US$5.5 million to settle a private class action involving the same conduct.

**10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?**

The Computer Fraud and Abuse Act and the Electronic Communications Privacy Act, as well as state surveillance laws, may come into play where cookies collect information from the computer on which they are placed and report that information to the entity placing the cookies without proper consent.

**10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?**

Yes, the FTC has brought regulatory enforcement actions against companies that failed to disclose or misrepresented their use of cookies.

**10.4 What are the maximum penalties for breaches of applicable cookie restrictions?**

Maximum fines are not set by statute.

## 11 Restrictions on International Data Transfers

**11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.**

The U.S. does not place restrictions on the transfer of personal data to other jurisdictions.

**11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).**

This is left to the discretion of the company, as the U.S. does not place restrictions on the transfer of personal data to other jurisdictions. With respect to receiving data from abroad, prior to *Schrems II*, the EU-US Privacy Shield Framework provided a mechanism to comply with data protection requirements when transferring personal data from the European Union to the United States. However, since the invalidation of the Privacy Shield Framework in *Schrems II*, the mechanisms to govern data transfers from the EU to the U.S. are limited largely to use of SCCs, BCRs, or derogations.

**11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.**

No such registration/notification is required.

**11.4 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?**

Although the FTC has not issued formal guidance following the decision in *Schrems II*, it has nevertheless provided an update stating that it continues "to expect companies to comply with their ongoing obligations with respect to transfers made under the Privacy Shield Framework", and encouraging those businesses to adhere to "robust privacy principles".

Additionally, the Department of Commerce, Department of Justice, and the Office of the Director of National Intelligence issued a White Paper in September 2020 that provides guidance in light of the *Schrems II* decision. This White Paper provides a framework to inform companies' assessment of the protections afforded by U.S. law in connection with relying on SCCs and advice to companies who have received orders authorised under FISA 702 requiring the disclosure of data to U.S. intelligence agencies.

**11.5 What guidance (if any) has/have the data protection authority(ies) issued in relation to the European Commission's revised Standard Contractual Clauses?**

While public authorities in the U.S. have not issued formal guidance in relation to the European Commission's draft revised SCCs, the U.S. did submit comments on the draft. The comments do not provide any specific guidance for companies, but rather reflect a concern that the draft revised SCCs may interfere with government efforts to protect public safety and national security along with joint US-EU cooperation on these issues. The U.S. also remains concerned with the ways that the draft revised SCCs create different standards for data requests by the U.S. government in comparison to similar requests from EU Member States.

## 12 Whistle-blower Hotlines

**12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?**

The federal Whistleblower Protection Act of 1989 protects federal employees, and some states have similar statutes protecting state employees. Public companies subject to the Sarbanes-Oxley Act also are required to have a whistle-blower policy which must be approved by the board of directors and create a procedure for receiving complaints from whistle-blowers.

**12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?**

Anonymous reporting generally is permitted. Rule 10A-3 of the Securities Exchange Act of 1934, for example, requires that audit committees of publicly listed companies establish procedures for the confidential, anonymous submission by employees of concerns regarding questionable accounting or auditing matters.

## 13 CCTV

**13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?**

The use of CCTV must comply with federal and state criminal voyeurism/eavesdropping statutes, some of which require signs to be posted where video monitoring is taking place, restrict the use of hidden cameras, or prohibit videotaping altogether if the location is inherently private (including places where individuals typically get undressed, such as bathrooms, hotel rooms and changing rooms).

**13.2 Are there limits on the purposes for which CCTV data may be used?**

There generally are no restrictions on the use of lawfully collected CCTV data, subject to a company's own stated policies or labour agreements.

## 14 Employee Monitoring

**14.1 What types of employee monitoring are permitted (if any), and in what circumstances?**

Employee privacy rights, like those of any individual, are based on the principle that an individual has an expectation of privacy unless that expectation has been diminished or eliminated by

context, agreement, notice, or statute. Monitoring of employees generally is permitted to the same extent as it is with the public, including when the employer makes clear disclosure regarding the type and scope of monitoring in which it engages, and subject to generally applicable surveillance laws regarding inherently private locations as well as employee-specific laws such as those regarding the privacy of union member activities.

**14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.**

Consent and notice rights are state-specific, as is the use of hidden cameras. When required or voluntarily obtained, employers typically obtain consent for employee monitoring through acceptance of employee handbooks, and may provide notice by appropriately posting signs.

**14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?**

The National Labor Relations Act prohibits employers from monitoring their employees while they are engaged in protected union activities.

## 15 Data Security and Data Breach

**15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?**

In the consumer context, the FTC has stated that a company's data security measures for protecting personal data must be "reasonable", taking into account numerous factors, to include the volume and sensitivity of information the company holds, the size and complexity of the company's operations, and the cost of the tools that are available to address vulnerabilities. Certain federal statutes and certain individual state statutes also impose an obligation to ensure security of personal information. For example, the GLBA and HIPAA impose security requirements on financial services and covered healthcare entities (and their vendors). Some states impose data security obligations on certain entities that collect, hold or transmit limited types of personal information. For example, the New York Department of Financial Services (NYDFS) adopted regulations in 2017 that obligate all "regulated entities" to adopt a cybersecurity programme and cybersecurity governance processes. The regulations also mandate reporting of cybersecurity events, like data breaches and attempted infiltrations, to regulators. Covered entities include those banks, mortgage companies, insurance companies, and cheque-cashers otherwise regulated by the NYDFS. Enforcement of the NYDFS regulation has begun, with the first fine of US$1.5 million issued in early 2021.

**15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

At the federal level, other than breach notification requirements pertaining to federal agencies themselves, HIPAA requires "Covered Entities" to report impermissible uses or disclosures that compromise the security or privacy of protected health information to the Department of Health and Human Services. Under the Privacy Rule, if the breach involves more than 500 individuals, such notification must be made within 60 days of discovery of the breach. Information to be submitted includes information about the entity suffering the breach, the nature of the breach, the timing (start and end) of the breach, the timing of discovery of the breach, the type of information exposed, safeguards in place prior to the breach, and actions taken following the breach, including notifications sent to impacted individuals and remedial actions.

While not specifically a data breach notification obligation, the Securities and Exchange Act and associated regulations, including Regulation S-K, require public companies to disclose in filings with the Securities and Exchange Commission when material events, including cyber incidents, occur. To the extent cyber incidents pose a risk to a registrant's ability to record, process, summarise and report information that is required to be disclosed in SEC Commission filings, management should also consider whether there are any deficiencies in its disclosure controls and procedures that would render them ineffective.

Some state statutes require the reporting of data breaches to a state agency or attorney general under certain conditions. The information to be submitted varies by state but generally includes a description of the incident, the number of individuals impacted, the types of information exposed, the timing of the incident and the discovery, actions taken to prevent future occurrences, copies of notices sent to impacted individuals, and any services offered to impacted individuals, such as credit monitoring.

**15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

At the federal level, HIPAA requires covered entities to report data breaches to impacted individuals without unreasonable delay, and in no case later than 60 days. Notice should include a description of the breach, including: the types of information that were involved; the steps individuals should take to protect themselves, including who they can contact at the covered entity for more information; as well as what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches. For breaches affecting more than 500 residents of a state or jurisdiction, covered entities must provide local media notice, in addition to individual notices.

As of May 2018, all 50 states, the District of Columbia, Guam, Puerto Rico and the U.S. Virgin Islands have statutes that require data breaches to be reported, as defined in each statute, to impacted individuals. These statutes are triggered by the exposure of personal information of a resident of the jurisdiction, so if a breach occurs involving residents of multiple states, then multiple state laws must be followed. Most statutes define a "breach of the security of the system" as involving unencrypted computerised personal information, but some states include personal information in any format. Triggering personal information varies by statute, with most including an individual's first name or first initial and last name, together with a data point, including the individual's Social Security Number, driver's licence or state identification card number, financial account number or payment card information. Some

states include additional triggering data points, such as date of birth, mother's maiden name, passport number, biometric data, employee identification number or username and password. The standard for when notification is required varies from unauthorised access to personal information, to unauthorised acquisition of personal information, to misuse of or risk of harm to personal information. Most states require notification as soon as is practical, and often within 30 to 60 days of discovery of the incident, depending on the statute. The information to be submitted varies by state but generally includes a description of the incident, the types of information exposed, the timing of the incident and its discovery, actions taken to prevent future occurrences, information about steps individuals should take to protect themselves, information resources, and any services offered to impacted individuals such as credit monitoring.

**15.4 What are the maximum penalties for data security breaches?**

Penalties are statute- and fact-specific. Under HIPAA, for example, monetary fines can range from US$100 to US$50,000 per violation (or per record), with a maximum penalty of US$1.75 million per year for each violation. By way of example, in 2020, the HHS and the attorneys general of 42 states entered into a US$39.5 million settlement with a health insurer in relation to a data breach affecting the health records of over 79 million individuals. Marking the current high point for enforcement, in 2019, a company agreed to pay a record penalty of at least US$575 million, and potentially up to US$700 million in a data breach settlement reached with the FTC, the CFPB, 48 states, the District of Columbia, and the Commonwealth of Puerto Rico.

## 16 Enforcement and Sanctions

**16.1 Describe the enforcement powers of the data protection authority(ies).**

The U.S. does not have a central data protection authority, as such, the enforcement powers of the regulators will depend on the specific statute in question. Some laws only permit federal government enforcement, some allow for federal or state government enforcement, and some allow for enforcement through a private right of action by aggrieved consumers. Whether the sanctions are civil and/or criminal depends on the relevant statute. For example, HIPAA enforcement permits the imposition of civil and criminal penalties. While HIPAA's civil remedies are enforced at the federal level by HHS, and at the state level by Attorneys General, the U.S. Department of Justice (USDOJ) is responsible for criminal prosecutions under HIPAA. At the state level the CPRA (amending the CCPA) created the California Privacy Protection Agency – the first dedicated data privacy regulator in the U.S. – to enforce consumer rights and business obligations under the CPRA.

(a) **Investigative Powers**: Depending on the applicable data protection laws, regulators in the U.S. may have the authority to conduct investigations into potential violations of data protection requirements.

(b) **Corrective Powers**: Depending on the applicable data protection laws, regulators in the U.S. may have the authority correct non-compliance actions of businesses through injunctive relief or under consent orders.

(c) **Authorisation and Advisory Powers**: Depending on the applicable data protection laws, regulators in the U.S. will often provide a method for businesses to consult with the regulators for additional and specific guidance.

(d) **Imposition of administrative fines for infringements of specified GDPR provisions**: This is not relevant for our jurisdiction.

(e) **Non-compliance with a data protection authority**: Depending on the applicable data protection laws, non-compliance with a data protection authority will generally attract renewed or additional enforcement against the business.

**16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?**

The U.S. does not have a central data protection authority. Enforcement authority, including whether a regulator may ban a particular processing activity, is specified in the relevant statutes. For example, 11 states have adopted the Insurance Data Security Model Law developed by the National Association of Insurance Commissioners. Among other things, these laws empower state insurance commissioners to issue cease-and-desist orders pertaining to data processing violations in the insurance industry, and even to suspend or revoke an insurance institution's or agent's licence to operate.

**16.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.**

In the U.S., this depends on the relevant statutory enforcement mechanism and the agency conducting the enforcement measures. The FTC, for example, in addition to publishing on its website all of the documents filed in FTC cases and proceedings, publishes an annual summary of key data privacy and data security enforcement actions and settlements, which provides guidance to businesses on its enforcement priorities. Similarly, HHS publishes enforcement highlights, summarises the top compliance issues alleged across all complaints and, by law, maintains a website that lists mandatorily reported breaches of unsecured protected health information affecting 500 or more individuals.

**16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?**

Extraterritorial enforcement of a U.S. law would depend on a number of factors, including whether the entity is subject to the jurisdiction of the U.S. courts, the impact on U.S. commerce and the impact on U.S. residents, among other factors.

## 17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

**17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?**

When made pursuant to Mutual Legal Assistance Treaties, information requests are typically processed through the USDOJ, which works with the local U.S. Attorney's Office and local law enforcement, prior to review by a federal judge and service on the U.S. company.

### 17.2 What guidance has/have the data protection authority(ies) issued?

Guidance is agency-specific, and there is no central data protection authority. By way of example, the FTC has issued guidance on a variety of issues including children's privacy, identity theft and telemarketing. Some state Attorneys General have also offered resources on their websites for victims of identity theft and for companies suffering data security breaches.

## 18 Trends and Developments

### 18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

The FTC remained active in regulating data security and privacy issues in 2020. Amidst the global pandemic, the FTC focused on ensuring companies providing videoconferencing platforms remained complied with data security and privacy obligations. To this end, in November 2020, the FTC entered into a settlement with videoconferencing company accused of participating in unfair and deceptive practices regarding user security. As part of the settlement agreement, the company must make changes to its security policies, continuously review its software updates for security flaws, and obtain biannual assessments of its security programs by an FTC-approved independent third party. This settlement is indicative of the changes that the FTC has made to improve its data security related orders. Their approach has been to (1) make the orders more specific, (2) increase accountability of third-party compliance assessors, and (3) require that data security concerns be elevated to companies' boards or other such governing bodies. In addition, the FTC's Commissioners have emphasised their commitment to pursuing enforcement actions against companies that engage in unfair or unreasonable privacy and data security practices. In doing so, however, the Commissioners have recognised the potential limits of their authority and have called on Congress to enact legislation supplementing these powers or, alternatively, a national privacy law that would be enforceable by the FTC.

In December 2020, the DOJ, acting upon the authorisations of the FTC, and the attorneys general of California, Illinois, North Carolina, and Ohio agreed to a settlement with a satellite television company to resolve a dispute as to the monetary award in relation to a judgment under the TCPA, FTC Act, and other federal and state telemarketing laws. The parties settled the dispute on penalties for US$210 million, only US$70 million less than the 2017 award imposed by the US District Court for the Central District of Illinois. HHS faced many challenges in 2020 relating to the COVID-19 pandemic. Due to rapid growth of the telehealth model, HHS necessarily provided flexibility in its enforcement of HIPAA to ensure continued access to healthcare. To this end, HHS issued NDEs (Notification of Enforcement Discretion) to healthcare providers so long as they exercised good-faith use of videoconferencing while providing telehealth services to patients. Nevertheless, Q3 and Q4 of 2020 saw the return of HHS's active enforcement with the regulator issuing a US$6.85 million penalty under HIPAA in relation to a malware attack that compromised the personal data of over 10.4 million people.

In addition, the U.S. Office of the Comptroller of the Currency (OCC), which regulates U.S. banks, issued an US$80 million fine following a major data breach in 2019. A hacker accessed the bank's computer systems through cloud-computing servers, exposing 140,000 social security numbers and 80,000 bank account numbers. OCC established that: (1) the bank had failed to establish effective risk management when it migrated its IT operations to the cloud; (2) the bank's internal audit mechanism had failed to identify numerous control weaknesses and gaps; and (3) the bank's Board of Directors had neglected to hold management accountable for these data security failures. The OCC considered this pattern of misconduct a violation of the Federal Reserve's Interagency Guidelines Establishing Information Security Standards.

State Attorneys General also played a key role in bringing enforcement actions under specific state laws in 2020. For example, in September, the Attorneys General from 42 states and the District of Columbia settled claims against a health insurer for a major 2014–2015 data breach, which affected more than 79 million individuals across the United States. The insurer agreed to pay US$39.5 million to resolve the federal and state statutory and civil claims.

Finally, in August 2020, the DOJ charged a ride-sharing company's Chief Security Officer with "obstruction of justice and misprision of a felony in connection with an alleged attempted cover-up of a 2016 data breach". Although this case is ongoing, its resolution will be a significant signal to inform company responses to data breaches.

### 18.2 What "hot topics" are currently a focus for the data protection regulator?

We anticipate that the following topics will remain hot over the next year: state-level consumer data privacy law initiatives will continue to proliferate as more states move laws through their legislatures, possibly driving action at the federal-level; issues surrounding the collection and protection of biometric information (especially in relation to student privacy); consumer access to financial relief and other remedies when their data protection rights are violated, even in the absence of a showing of harm; and an increased focus by legislators and regulators alike on cybersecurity issues, particularly in the wake of data breaches involving significant technology vendor software.

**F. Paul Pittman** is Counsel in White & Case's international Data, Privacy & Cybersecurity legal practice. Paul advises global clients on the complex data protection and cybersecurity use and compliance issues that often arise in the processing of consumer and business data, and in the management of information and operational technology systems.

Paul's practice includes advising companies on cybersecurity risks and compliance, and guiding companies in responding to data breaches. Paul also assists clients in resolving data privacy and cybersecurity issues in business operations and products, including relating to connected devices (IoT) and FinTech. In addition, Paul advises global clients on all data privacy and cybersecurity matters that arise in corporate transactions.

Paul received a Bachelor of Science degree from Allegheny College, and a *Juris Doctor* degree from Washington and Lee University School of Law.

**White & Case LLP**
701 Thirteenth Street, NW
Washington, D.C. 20005-3807
USA

Tel: +1 202 729 2395
Email: paul.pittman@whitecase.com
URL: www.whitecase.com

**Kyle Levenberg** is an Associate in White & Case's international Data, Privacy & Cybersecurity legal practice. Kyle advises White & Case's global clients on the complex issues that often arise in the handling of consumer and business data under state, federal, and international laws and standards.

Kyle's practice includes guiding companies in developing and implementing creative and strategic privacy and cybersecurity compliance programmes. In addition, Kyle assists clients in resolving privacy and cybersecurity issues in business operations and products. Finally, Kyle also advises global clients on all privacy and cybersecurity matters that arise in corporate transactions, with a particular focus on buy-side mergers and acquisitions, initial public offerings and SPAC transactions.

Kyle holds a Bachelor of Laws from the University of Auckland and a *Juris Doctor* and Master of Laws from Duke University. Kyle is an active member of the International Association of Privacy Professionals (IAPP) and is CIPP/US qualified.

**White & Case LLP**
701 Thirteenth Street, NW
Washington, D.C. 20005-3807
USA

Tel: +1 202 729 2369
Email: kyle.levenberg@whitecase.com
URL: www.whitecase.com

# ICLG.com

## Other titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Cybersecurity
Derivatives
Designs
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Environmental, Social & Governance Law
Family Law
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Technology Sourcing
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

@ICLG_GLG

The International Comparative Legal Guides are published by:

global legal group