



# ICLG

## The International Comparative Legal Guide to: **Data Protection 2018**

### **5th Edition**

A practical cross-border insight into data protection law

Published by Global Legal Group, with contributions from:

Affärsadvokaterna i Sverige AB  
Anderson Möri & Tomotsune  
Ashurst Hong Kong  
BSA Ahmad Bin Hezeem & Associates LLP  
Clyde & Co  
Cuatrecasas  
DQ Advocates Limited  
Ecija Abogados  
Firat İzgi Attorney Partnership  
GANADO Advocates  
GÖRG Partnerschaft von Rechtsanwälten mbB  
Herbst Kinsky Rechtsanwälte GmbH  
Holding Redlich  
Jackson, Etti & Edu  
King & Wood Mallesons  
Koushos Korfiotis Papacharalambous LLC  
KPMG Law Firm  
Lee & Ko  
Loyens & Loeff Luxembourg S.à r.l.

Loyens & Loeff N.V.  
LPS L@w  
Lydian  
Mori Hamada & Matsumoto  
Naschitz, Brandes, Amir & Co., Advocates  
OLIVARES  
OrionW LLC  
Osler, Hoskin & Harcourt LLP  
Pachiu & Associates  
Pestalozzi Attorneys at law  
Pillsbury Winthrop Shaw Pittman LLP  
Rato, Ling, Lei & Cortés – Advogados  
Rossi Asociados  
Subramaniam & Associates (SNA)  
Trevisan & Cuonzo Avvocati  
Vaz E Dias Advogados & Associados  
White & Case LLP  
Wikborg Rein Advokatfirma AS



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

**Sales Director**  
Florian Osmani

**Account Director**  
Oliver Smith

**Sales Support Manager**  
Toni Hayward

**Sub Editor**  
Oliver Chang

**Senior Editors**  
Suzie Levy  
Caroline Collingwood

**Chief Executive Officer**  
Dror Levy

**Group Consulting Editor**  
Alan Falach

**Publisher**  
Rory Smith

**Published by**  
Global Legal Group Ltd.  
59 Tanner Street  
London SE1 3PL, UK  
Tel: +44 20 7367 0720  
Fax: +44 20 7407 5255  
Email: [info@glgroup.co.uk](mailto:info@glgroup.co.uk)  
URL: [www.glgroup.co.uk](http://www.glgroup.co.uk)

**GLG Cover Design**  
F&F Studio Design

**GLG Cover Image Source**  
iStockphoto

**Printed by**  
Ashford Colour Press Ltd  
June 2018

Copyright © 2018  
Global Legal Group Ltd.  
All rights reserved  
No photocopying

ISBN 978-1-912509-15-7  
ISSN 2054-3786

**Strategic Partners**



## General Chapters:

1	<b>The Rapid Evolution of Data Protection Laws</b> – Dr. Detlev Gabel & Tim Hickman, White & Case LLP	1
2	<b>Artificial Intelligence Policies in Japan</b> – Takashi Nakazaki, Anderson Mōri & Tomotsune	6

## Country Question and Answer Chapters:

3	<b>Australia</b>	Holding Redlich: Trent Taylor & Daniel Clarkin	11
4	<b>Austria</b>	Herbst Kinsky Rechtsanwälte GmbH: Dr. Sonja Hebenstreit & Dr. Isabel Funk-Leisch	20
5	<b>Belgium</b>	Lydian: Bastiaan Bruyndonckx & Olivia Santantonio	30
6	<b>Brazil</b>	Vaz E Dias Advogados & Associados: José Carlos Vaz E Dias	41
7	<b>Canada</b>	Osler, Hoskin & Harcourt LLP: Adam Kardash & Patricia Kosseim	54
8	<b>Chile</b>	Rossi Asociados: Claudia Rossi	66
9	<b>China</b>	King & Wood Mallesons: Susan Ning & Han Wu	73
10	<b>Cyprus</b>	Koushos Korfiotis Papacharalambous LLC: Loizos Papacharalambous & Anastasios Kareklas	83
11	<b>France</b>	Clyde & Co: Benjamin Potier & Jean-Michel Reversac	93
12	<b>Germany</b>	GÖRG Partnerschaft von Rechtsanwälten mbB: Dr. Katharina Landes	103
13	<b>Hong Kong</b>	Ashurst Hong Kong: Joshua Cole & Hoi Tak Leung	113
14	<b>India</b>	Subramaniam & Associates (SNA): Hari Subramaniam & Aditi Subramaniam	126
15	<b>Isle of Man</b>	DQ Advocates Limited: Sinead O'Connor & Hazel Dawson	139
16	<b>Israel</b>	Naschitz, Brandes, Amir & Co., Advocates: Dalit Ben-Israel & Efrat Artzi	149
17	<b>Italy</b>	Trevisan & Cuonzo Avvocati: Julia Holden & Benedetta Marsicola	158
18	<b>Japan</b>	Mori Hamada & Matsumoto: Hiromi Hayashi & Rina Shimada	169
19	<b>Korea</b>	Lee & Ko: Kwang Bae Park & Hwan Kyoung Ko	179
20	<b>Luxembourg</b>	Loyens & Loeff Luxembourg S.à r.l.: Véronique Hoffeld & Florence D'Ath	188
21	<b>Macau</b>	Rato, Ling, Lei & Cortés – Advogados: Pedro Cortés & José Filipe Salreta	198
22	<b>Malta</b>	GANADO Advocates: Dr. Paul Micallef Grimaud & Dr. Philip Mifsud	208
23	<b>Mexico</b>	OLIVARES: Abraham Diaz & Gustavo Alcocer	218
24	<b>Netherlands</b>	Loyens & Loeff N.V.: Kim Lucassen & Iram Velji	226
25	<b>Nigeria</b>	Jackson, Etti & Edu: Ngozi Aderibigbe	238
26	<b>Norway</b>	Wikborg Rein Advokatfirma AS: Line Coll & Vilde Juliussen	248
27	<b>Portugal</b>	Cuatrecasas: Sónia Queiróz Vaz & Ana Costa Teixeira	260
28	<b>Romania</b>	Pachiu & Associates: Mihaela Cracea & Alexandru Lefter	272
29	<b>Senegal</b>	LPS L@w: Léon Patrice Sarr	282
30	<b>Singapore</b>	OrionW LLC: Winnie Chang	290
31	<b>Spain</b>	Ecija Abogados: Carlos Pérez Sanz & Pia Lestrade Dahms	299
32	<b>Sweden</b>	Affärsadvokaterna i Sverige AB: Mattias Lindberg & Marcus Lorentzon	310
33	<b>Switzerland</b>	Pestalozzi: Lorenza Ferrari Hofer & Michèle Burnier	320
34	<b>Taiwan</b>	KPMG Law Firm: Lawrence Ong & Kelvin Chung	330
35	<b>Turkey</b>	Firat İzgi Attorney Partnership: Elvan Sevi Firat & Doğan Doru Alkan	338
36	<b>United Arab Emirates</b>	BSA Ahmad Bin Hezeem & Associates LLP: Rima Mrad & Nadim Bardawil	346
37	<b>United Kingdom</b>	White & Case LLP: Tim Hickman & Matthias Goetz	359
38	<b>USA</b>	Pillsbury Winthrop Shaw Pittman LLP: Deborah Thoren-Peden & Catherine D. Meyer	368
*	<b>Ireland</b>	Matheson: Anne-Marie Bohan (online only, see <a href="http://www.iclg.com">www.iclg.com</a> )	

Further copies of this book and others in the series can be ordered from the publisher. Please call +44 20 7367 0720

### Disclaimer

This publication is for general information purposes only. It does not purport to provide comprehensive full legal or other advice. Global Legal Group Ltd. and the contributors accept no responsibility for losses that may arise from reliance upon information contained in this publication. This publication is intended to give an indication of legal issues upon which you may need advice. Full legal advice should be taken from a qualified professional when dealing with specific situations.

## EDITORIAL

---

Welcome to the fifth edition of *The International Comparative Legal Guide to: Data Protection*.

This guide provides corporate counsel and international practitioners with a comprehensive worldwide legal analysis of the laws and regulations relating to data protection.

It is divided into two main sections:

Two general chapters. These are designed to provide readers with an overview of key issues affecting data protection, both from a multi-jurisdictional perspective and with a particular insight into artificial intelligence policies in Japan.

Country question and answer chapters. These provide a broad overview of common issues in data protection laws and regulations in 37 jurisdictions.

All chapters are written by leading data protection lawyers and industry specialists and we are extremely grateful for their excellent contributions.

Special thanks are reserved for the contributing editors Tim Hickman and Dr. Detlev Gabel of White & Case LLP for their invaluable assistance.

Global Legal Group hopes that you find this guide practical and interesting.

The *International Comparative Legal Guide* series is also available online at [www.iclg.com](http://www.iclg.com).

Alan Falach LL.M.  
Group Consulting Editor  
Global Legal Group  
[Alan.Falach@glgroup.co.uk](mailto:Alan.Falach@glgroup.co.uk)

## PREFACE

---

It is a pleasure to have been asked to provide the preface to *The International Comparative Legal Guide to Data Protection 2018*. 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 37 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 Brazil, Hong Kong, Luxembourg, Netherlands, Nigeria and the United Arab Emirates, which reflects the growth of privacy compliance requirements and challenges in an increasing number of jurisdictions worldwide. As with other entries in the ICLG series, this edition will provide a go-to resource for anyone seeking practical guidance on these complex international legal issues.

Tim Hickman  
Partner  
White & Case LLP

# The Rapid Evolution of Data Protection Laws

White & Case LLP

Dr. Detlev Gabel



Tim Hickman



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 organisations 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 all 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 aging 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 drafted and finalised Regulation (EU) 2016/679 (the General Data Protection Regulation, or “**GDPR**”). The GDPR marks the biggest single shift in data protection laws in Europe since Directive 95/46/EC (the “**Directive**”) was finalised in 1995. The GDPR was published on 4 May 2016, marking the end of a four-year legislative process. It introduces a raft of sorely needed clarifications and updates, which is intended to carry EU data protection law forward, well into the next decade. It also introduces major changes to the compliance burden borne by organisations.

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 will necessarily be engaged in the processing of personal data (e.g., every time an email is sent or received). For many businesses, the GDPR will impact almost every area of operations, from marketing to IT, from human resources to procurement. Anywhere that information about people is handled, the GDPR will follow 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 located 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 (for example, 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 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 such an 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 will need to do so in accordance 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 existing data protection laws in the EU 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. In addition, in the event that penalties are issued in respect of a breach of EU data protection law, the level of such penalties has traditionally been comparatively low. 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 raises the bar for compliance significantly. It requires greater openness and transparency – the level of detail that businesses are required to disclose in policies and notices regarding their processing activities has significantly increased. The GDPR imposes tighter 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 more powerful rights to enforce against businesses. Some of these rights (e.g., the right of individuals to gain access to their personal data, and to be informed about how those data are being used) are simply expansions of existing rights, and can largely be addressed with existing compliance measures developed under the Directive. Others (such as 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) are new, and require fresh thinking from businesses.

Satisfying these requirements will prove 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 access 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 ongoing. It should also be noted that certain provisions of the GDPR require national implementation in each EU Member State, meaning that there will 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.

Looking to the future, the EU is in the process of finalising the ePrivacy Regulation – a law that will 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. While the final text of the ePrivacy Regulation is still some way off, it is clear that the 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.

### 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 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) are updating 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 Argentina are in the process of revising their local data protection laws to implement standards that will more closely match the GDPR. 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 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, at the start of 2017, the EU opened talks with Japan regarding the possibility of a mutual adequacy decision, designed to allow bilateral data flows without the need for additional safeguards. It is hoped that these discussions will be concluded in 2018. However, there are significant differences in content and principle between the GDPR and Japan’s domestic data protection laws, as well as culturally distinct approaches to the concept of privacy. Nevertheless, there is optimism that a deal can be reached.

Meanwhile, many jurisdictions are in the process of implementing new comprehensive national data protection compliance requirements. 2018 sees new registration deadlines imposed in the Philippines for businesses that process personal data, and is expected to see new compliance obligations for both the private sector and the public sector in Mexico. South Africa’s POPIA law has been on the statute books for several years now, but its entry into force has been delayed for a variety of political and budgetary reasons. Nevertheless, it is expected that enforcement of POPIA will begin in earnest in the near future. Turkey has also made recent strides, with the creation of a national data protection authority, and new data protection legislation in the last couple of years. 2018 will bring new guidelines and enforcement decisions that are expected to provide clarity on the obligations of businesses that process personal data in Turkey.

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. In the last year we have seen new cybersecurity laws introduced in China, where new national data security standards have been issued, and enforcement has already begun. Likewise, we have seen the introduction of information security regulations in Israel, which incorporate data breach reporting requirements. Singapore has also passed a new cybersecurity law, with the aim of enhancing security in Critical Information Infrastructure (“**CII**”). This law, which is in some respects similar to the NIS Directive, focuses on cybersecurity in key sectors including finance, energy and healthcare. The new law requires operators of CII to adhere to pre-determined cybersecurity standards and to report cyber breaches to the relevant authorities. In parallel, Singapore is updating its privacy legislation to include mandatory data breach reporting obligations.

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 data to 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. Within the EU, there is pressure for all such localisation requirements to be removed, to allow the truly free flow of data within the EU. However, in a number of other parts of the world, data localisation laws are becoming increasingly popular, and in some cases are being used as a means of digital protectionism.

### Future Uncertainty

Perhaps the greatest area of future uncertainty at the time of writing is Brexit. While Brexit 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. But once the UK formally ceases to be an EU Member State, it will become a “third country” for the purposes of EU law. In particular, the UK will not automatically be treated as having sufficiently protective 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 indicated that it will retain the GDPR in full, in its national laws, meaning that there will, in principle, be complete equivalency between data protection laws that apply in the EU and data protection laws that apply in the UK after Brexit. In addition, it is unlikely that the UK will impose meaningful barriers to the transfer of personal data from the UK to the EU after Brexit. However, as noted above, it is the transfer of data in the opposite direction (from the EU to the UK) that is likely to pose a thornier challenge.

One obvious way out of this dilemma would be for the European Commission to grant the UK an adequacy decision. On the one hand, this seems like a logical outcome, since the UK will have essentially identical data protection laws to the EU, and is therefore arguably the jurisdiction that is most deserving of an adequacy decision, from a pure legal analysis perspective. On the other hand, it is not yet certain whether the UK will be granted an adequacy decision because, from a political perspective, a large amount remains to be decided in the course of the Brexit negotiations. In particular, the UK’s approach to surveillance and counterterrorism, the active and in-depth collection and retention of communications data in the UK for security purposes, and the UK’s membership of certain international intelligence-sharing organisations, has led to suggestions from some quarters that, after Brexit, the UK’s approach to privacy and data protection will no longer be consistent with the EU’s approach to these issues, making the granting of an adequacy decision more complex than it might first appear.

A further area of uncertainty is the manner in which the GDPR will be enforced. While the mechanisms for enforcement, and the powers of the regulators, are reasonably clear, there is significant doubt in some areas. First, Article 83 of the GDPR (which sets out the maximum penalties applicable to certain types of breaches under the GDPR) is silent on the issue of who can receive penalties under the GDPR. Whereas the Directive explicitly refers to powers used to admonish controllers, the GDPR appears to leave open the possibility that penalties could be applied to both controllers and processors, where they are involved in a breach of the GDPR. This change has serious implications for service provider businesses that

act as processors, which were previously relatively insulated from the risk of regulatory enforcement under the Directive. However, the potential compliance risk under the GDPR goes one step further. Article 83 refers to the concept of an “undertaking”, for the purposes of calculating penalties based on percentages of turnover. 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.

Notwithstanding the risks in relation to financial penalties under the GDPR, it also 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 mid-1990s 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 facial 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 about machine learning and artificial intelligence? 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 position in the EU, and certain other jurisdictions, is now settled for the foreseeable future, but lawmakers in jurisdictions where privacy is an emerging theme 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 users, 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 outright prohibit 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, artificial intelligence 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 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 GDPR compliance unless they are required to do so. Therefore, it is generally advisable to ensure that responsibility for 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 the GDPR 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 take those issues seriously. 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**

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

Tel: +49 6929 9940  
Email: [dgabel@whitecase.com](mailto:dgabel@whitecase.com)  
URL: [www.whitecase.com](http://www.whitecase.com)

Detlev is a partner in the Frankfurt office of White & Case and head of the Firm's EMEA Data, Privacy & Cyber Security Practice.

Detlev advises multinational clients on a broad range of data protection and data security matters, including European and German data protection law compliance, cross-border data transfers and information governance issues.

Detlev frequently publishes and speaks on topics relating to the aforementioned areas. Notably, he is the co-editor and co-author of a treatise on German data protection law and lectures on data protection law at the University of Oldenburg, Germany, in a course leading to a Master of IT Law.

The legal directories consistently list him as a leading individual for data protection law in Germany.

**Tim Hickman**

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

Tel: +44 7532 2517  
Email: [tim.hickman@whitecase.com](mailto:tim.hickman@whitecase.com)  
URL: [www.whitecase.com](http://www.whitecase.com)

Tim advises on all aspects of UK and EU privacy and data protection law, from general compliance issues (such as implementing privacy policies and consent forms) to more specialised issues (such as managing data breaches, structuring cross-border data transfers and complying with the "right to be forgotten"). Tim has a detailed knowledge of the EU's General Data Protection Regulation, and co-authored White & Case's Handbook on that legislation ([www.whitecase.com/eu-gdpr-handbook](http://www.whitecase.com/eu-gdpr-handbook)).

Clients appreciate Tim's ability to find pragmatic and commercial solutions to complex (and frequently multi-jurisdictional) data protection compliance questions.

Tim has significant experience of working with a wide range of clients in the EU, the US and Asia. He has also spent time on secondment at Google, advising on cutting-edge privacy and data protection issues.

## WHITE & CASE

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, manufacturing and electronics, publishing and media.



# Artificial Intelligence Policies in Japan

Anderson Mōri & Tomotsune

Takashi Nakazaki



## 1 Trends in Artificial Intelligence in Japan

- In December 2014, the Japanese Society for Artificial Intelligence (JSAI) established the Ethics Committee to discuss and consider the relationship between artificial intelligence (AI) and society. Thereafter, in February 2017, the JSAI released the Ethical Guidelines.
- Acceptable Intelligence with Responsibility (AIR) is a scholarly group wherein researchers in fields such as science, technology and society (STS) and AI discuss social acceptance of AI. In furtherance of their discussions, researchers in the group visit locations where AI is accepted and interview people who are involved in furthering the social acceptance of AI.
- The Information Network Law Association's study group on robot law is investigating international research trends concerning social institutions and consumer protection.
- In February 2016, the Ministry of Internal Affairs and Communications set up The Committee for AI Networking to evaluate the impacts and risks of AI networking to society and the economy. The Committee for AI Networking then released the principles for AI R&D, which are discussed in more detail in section 3 of this chapter. Since October 2016, the committee has continued making guidelines for AI R&D.
- The Fifth Science and Technology Basic Plan was formulated by the Council for Science, Technology and Innovation (CSTI) and put into action in 2016. Emphasising the importance of technology innovation and deepening the relationship between society and science, the plan implements a long-term systematic and consistent science and technology policy. It recognises that AI technology is an important part of realising Society 5.0, which is a future society of highly integrated technology envisioned in a Japanese government policy.
- Japan aims to achieve Society 5.0 in the future through the full utilisation of technological innovation including the Internet of Things (IoT), AI and big data derived from the fourth industrial revolution. To achieve Society 5.0, industries must play a key role. In light of this, the Japanese government has announced Connected Industries as a new conceptual framework. Under this framework, industries will add value and create new solutions to various societal problems by connecting various features of modern life, including humans (including our roles as consumers and suppliers), machines, systems and companies. To this end, the Japanese government is advancing a wide variety of policy initiatives in cooperation with private sector parties. With respect to those initiatives, the following three reports are especially important.

## 2 Report on Artificial Intelligence and Human Society

This report was issued by the Advisory Board on Artificial Intelligence and Human Society in March 2017. The Board has been supported by the Ministry of Internal Affairs and Communication. The report identifies the key issues which benefit and empower human society and contribute to ensuring society's sustainability.

### 2.1 Ethical issues

#### 2.1.1 The possibility that AI technologies will be used to manipulate emotion, faith and behaviour and make ranking or selections without awareness causes concern

AI technologies are becoming capable of making decisions and taking actions that previously only humans were able to perform. Many people are concerned about the potential for AI to be used to manipulate or control their minds and behaviour and to influence their emotions, affections and faith. There are also concerns about the evaluation or ranking of people by AI technologies. If AI technologies are used in this fashion without the awareness of society, ethical discussions might become critically important.

#### 2.1.2 Revisiting the concept of humanity

The future blueprints of AI show that AI technologies augment human senses and abilities with respect to space, time and the body. With the prospect of AI augmenting human senses, there is an opportunity to revisit the concept of humanity by considering the potential of AI.

### 2.2 Legal issues

#### 2.2.1 When considering the risks of using AI technologies, clarifying responsibility and utilising insurance is important

Consideration of the applicable legal issues accelerates the acceptance and safe use of AI technology by society. Previously, statistical reports showed that most traffic accidents were caused by human errors and carelessness. Consequently, the use of autonomous cars creates the expectation that traffic accidents will decrease and society will be safer. However, the use of autonomous cars creates new issues such as who is responsible for accidents caused by autonomous car systems.

Society's newly implemented AI technologies require a clear determination to be made regarding who is responsible for the associated risks, accidents, rights infringement, benefits and achievements. This determination is important in preventing

businesses from becoming intimidated by or overreacting to reputational risks arising from the use of AI technologies. In making such determination, it also might be useful to allocate responsibility according to the levels of technological advancement (e.g., levels 0 to 4 for automated driving technology) and to handle uncertain, probable risks through insurance.

Likewise, in considering potential legal issues, it is important to discuss the possibility of lost opportunities and credibility as a result of not using AI technologies. For example, corporate managers are obligated to conduct the affairs of the company with the care required of a prudent manager. By utilising AI, a corporate manager can collect and analyse an exponentially larger amount of useful information related to corporate management in a shorter amount of time than before the use of AI. In such circumstances, declining AI might result in a judgment that the manager has failed to perform his/her duties with the due care of a prudent manager.

The implications of using or not using AI are fact-dependent and the facts are likely to change rapidly. Therefore, the use of AI and the associated ramifications must be carefully considered from all angles.

### **2.2.2 Exploitation of big data while considering information privacy protection**

The ability to exploit big data makes AI technologies more useful. Nevertheless, the increased usefulness of AI technologies must be balanced against privacy concerns. Consequently, it is necessary to consider appropriate institutional frameworks (laws, guidelines and contracts) to avoid the chilling effects of privacy invasion.

Our society must discuss access rights to personal information data, data portability and related security issues on an international scale. Additionally, it has been suggested that these issues should be embodied in the government services which are based on AI technologies. Japan's Act on Protection of Personal Information, however, does not stipulate that users have the right to avoid automated decisions by computer programmes including AI regarding their legal rights and other similar important rights based on their profiles. Nevertheless, there has been some discussion about introducing into the Act a provision similar to that in the General Data Protection Rules (GDPR) within several years which would remedy that deficit.

### **2.2.3 Considering the rights and incentives associated with products created by AI technologies**

The exploitation of AI technologies encourages the easy creation of high-value products by algorithm developers, learned-data providers, service providers, final creators and others. Consequently, it is necessary to consider who retains the property rights to a creation or a learned model produced by either AI technologies or the collaboration between AI technologies and humans (i.e., issues of data ownership).

Furthermore, to facilitate the development and utilisation of AI technologies, society must find an appropriate method to assign rights (incentives) to algorithm developers, algorithm users and data providers by means of appropriate contracts and guidelines. These issues should be covered by contracts among the relevant parties. For that reason, the AI Data Related Contracts Guidelines (Chapter 4) specifies some points to be considered and stipulated by such contracts.

### **2.2.4 Interpretation and revision of laws and the basic science underlying legal concepts**

Ongoing discussions about employment changes caused by AI technologies contribute to appropriate revisions to the applicable laws on transportation, business, medicine, labour, etc. These discussions raise the possibility that underlying legal concepts, such as human responsibility, will be fundamentally changed. For example, the existing laws do not clearly allocate responsibility for the products created by either AI technologies or the collaboration

of humans and AI technologies. Since AI technologies based on machine-learning are socially implemented, the acceptance of AI technologies requires human society to advance along with the technologies. Thus, the fundamental concepts on which modern laws are based, such as human responsibility, must be reconsidered.

## **2.3 Social issues**

### **2.3.1 Freedom to use (or not use) AI technologies and people's dialogue on common social values**

The numerous social benefits from AI technologies include things such as the realisation of social security and safety, the improvement of productivity to counter labour shortages, a decreasing birthrate and an aging population, and the facilitation of participation by various people (inclusiveness) with individually optimised AI technology. Thus, AI technologies are crucial to the realisation of Society 5.0. However, like many other tools and technologies, the utilisation of AI technologies cannot be socially enforced.

It may be necessary to consider the need to ensure the freedom to use AI technologies in light of an individual's faith. AI technologies work as a part of information technology (IT) or software programmes, so users cannot simply confirm that AI services/products are being used. Thus, a discussion is required about whether users should always be notified that AI technologies are being used. Furthermore, Society 5.0 demands the avoidance of social conflicts between AI services/products users and non-users. This also requires an ongoing dialogue among people with different visions and ideas, including experts, in order to consider opposing opinions regarding fundamental social values.

### **2.3.2 The AI divide: the unbalanced social costs relative to AI; and the prevention of discrimination**

To maximise the benefits from AI technologies, users need digital goods and services literacy and knowledge about data privacy and the AI technologies themselves. However, all people cannot acquire or maintain sufficient knowledge and literacy. This inability might be a causal factor in the so-called "AI divide."

For example, "rideshare", which is backed by AI optimisation technologies, could offer a new means of transport that is less expensive than taxis and is supportive of socially disadvantaged people. However, access to rideshare services requires a minimum familiarity with digital devices. Consequently, those without digital literacy may be excluded from the benefit of rideshare services. And, as ridesharing increases in popularity, the traditional taxi services may decrease or become prohibitively expensive. Therefore, the AI divide must be considered when making policies to avoid creating an imbalance in social costs due to differences in digital literacy, knowledge and assets. Potential discrimination based on the output of personal profiling by AI technologies must be prevented.

### **2.3.3 New social pathology, conflict and dependence on AI technologies**

With increasing opportunities to use AI technologies in social contexts, there is a possibility of generating new social problems, such as excessive rejection, overconfidence and dependence on AI technologies. Recommendations and personal optimisation by AI technologies may limit the information available to individuals and increase the tendency for people to regard the limited information as universal. It is, therefore, necessary to provide accurate information and opportunities for dialogue and training.

## **2.4 Research and development issues**

### **2.4.1 Ethics, accountability and visualisation**

Researchers and engineers are required to engage in R&D in

AI-related areas with a high level of professional ethics while simultaneously observing and being accountable for the ethical codes and guidelines of their academic societies and organisations. AI technologies have features which are widely unknown to users. In other words, individuals use products/services without knowing how the technology included therein actually works. Thus, when conducting R&D, it is recommended to visualise how AI technologies are used in decisions and actions.

#### **2.4.2 Security, privacy protection, controllability and transparency**

Scientists and engineers are required to establish environments for the use of AI technologies which have robust cyber-security and safety features. It is especially essential to develop technology that enables users to choose how much personal data to share, the level of individual privacy to be protected and what kind of information can be used publicly. R&D should be conducted to develop technologies that enable people to control the safety features of AI technologies, to explain the logic and process of the calculations used by AI technologies and to provide interfaces which smoothly transition control from the AI to the user, especially in emergencies.

#### **2.4.3 Appropriate disclosure of information: promoting the humanities; social sciences; and research collaboration**

AI technologies based on machine-learning produce statistically valid outputs and statistically benefit society. Nevertheless, for this paradigm to be accepted in society, scientists and engineers are required to explain it appropriately. Thus, when promoting new technologies, researchers and engineers might have to explain their benefits and risks fairly.

To discuss the relationship between AI technologies and society adequately and to design and realise a better future society, researchers in the humanities and social sciences should acquire up-to-date knowledge of new technologies and utilise them in their research. Scientists and engineers should also collaborate with researchers in the humanities and social sciences to pursue socially beneficial AI technologies.

#### **2.4.4 Diversity of AI technologies for social diversity**

While AI technologies are currently advancing in deep-learning and machine-learning, there are various basic theories and technologies. In the future, new theories will emerge and further promote AI technologies. The government needs to promote basic sciences and create an environment that supports open science to enhance R&D in AI technology diversity. This will contribute to the advancement, robustness and safety of AI technologies. Such technological diversity seems suited for social diversity.

### **2.5 Educational issues**

#### **2.5.1 Cultivating individuals' ability to utilise AI technologies**

AI services/products work appropriately if users understand their benefits and risks, learn how to identify responsibilities and operate them perfectly to keep them under control. It is necessary to understand the advantages and limits of the current AI technologies, to perfectly utilise AI technologies and to perform creative activities in collaboration with AI technologies.

#### **2.5.2 Enhancing essential human abilities that AI technologies cannot perform**

Education policy is created based on discussions about the limitations of technologies. For example, a deep understanding of semantics, the utilisation of experience-based imagination in novel situations, the ability to identify a problem that should be solved, the ability to communicate and collaborate and the ability to explore novel information actively and to discuss and incorporate the opinions of

others are all abilities that current machine-learning AI technologies seem unable to perform. Education for children is especially urgent because it takes time, and the development of AI technologies is so rapid. It is important to consider what abilities should be still learned by humans for proper brain development even though the activities enabled by said digital abilities can be performed instead by AI technologies.

### **2.6 Economic Issues**

#### **2.6.1 Industrial policies facilitating AI technology utilisation, and educational and employment policies enabling labour mobility**

At the government level, it is necessary to formulate policies that provide opportunities for people to learn skills that enable labour mobility through AI technologies. Labour mobility will facilitate economic growth and ensure that there is a variety of work styles suitable for individuals. The government also must assist in determining how to harmonise an individual's abilities with a creative job/task.

Combining educational and employment policies is one method to enable labour movement. In addition, the government's perspective on macroeconomic policies and safety nets must be appropriate. The procedures to fairly distribute profits from AI services/products, economic revitalisation and the prevention of economic disparities should be proposed after considering the benefits of AI systems. Since AI technologies would be beneficial to addressing Japan's labour shortage, policies that enhance industrial competitiveness should be accelerated. Those policies will be more effective if users provide their opinions about companies' activities and the government's policies.

## **3 Draft AI R&D Guidelines for International Discussion**

In July 2017, the Conference Toward AI Network Society, which was supported by the Ministry of Internal Affairs and Communication, issued a draft which proposed nine principles (the "Principles"). In sum, Principle #1 is primarily directed at developing sound AI networking and promoting the benefits of AI systems. By contrast, Principles #2–#7 are directed at mitigating the risks associated with AI systems, and Principles #8 and #9 are directed at improving user acceptance. The specific details about the Principles are set forth below.

**#1 Principle of collaboration** – Developers should pay attention to the interconnectivity and interoperability of AI systems.

Developers should consider the interconnectivity and interoperability between the AI systems that they have developed and other AI systems, as well as the diversity of AI systems in general. As a result of such consideration, (a) the benefits of AI systems should increase through the sound progress of AI networking, and (b) the efforts of multiple developers to control the risks can be coordinated to operate effectively. In particular, developers should consider the following points:

- Cooperating to share relevant information which is effective in ensuring interconnectivity and interoperability of AI systems.
- The development of AI systems which conform to international standards, if any.
- The standardisation of data formats and the openness of interfaces and protocols including application programming interfaces (API).
- Awareness of the risks of unintended events as a result of the interconnection or interoperations of AI systems.

- The promotion of open and fair treatment of licence agreements for intellectual property rights and the terms thereof, such as standard essential patents, which considers the balance between the protection and utilisation of intellectual property related to the development of AI.

**#2 Principle of transparency** – Developers should focus on the verifiability of the inputs/outputs of AI systems and their ability to explain the judgments of the AI systems.

The AI systems subject to the principle of transparency are those which might affect the life, body, freedom, privacy or property of users or third parties. Developers, therefore, should focus on the verifiability of the inputs and outputs of AI systems as well as their ability to explain the judgments of AI systems within a reasonable scope given the characteristics of the technologies to be adopted and their use. By focusing on these issues, developers can obtain the understanding and trust of AI system users.

**#3 Principle of controllability** – Developers should pay attention to the controllability of AI systems.

In order to assess the risks related to the controllability of AI systems, developers are encouraged to verify and validate the controllability of AI systems in advance. One possible method of risk assessment is to conduct experiments of the AI system in a closed space, such as a laboratory in which security is ensured, prior to its use by society. In addition, in order to ensure the controllability of AI systems, developers are encouraged to confirm, to the extent possible, that supervision (such as monitoring or warnings) and countermeasures (such as system shutdowns, isolation from other networks or repairs) by humans or other trustworthy AI systems are effective in light of the characteristics of the technologies to be adopted.

**#4 Principle of safety** – Developers should ensure that AI systems will not harm the life, body or property of users or third parties through actuators or other devices.

The AI systems subject to the principle of safety are those which might harm the life, body or property of users or third parties through actuators or other devices. Developers are encouraged to reference relevant international standards and focus on the following considerations given the possibility that outputs or programmes might change as a result of learning or other actions of AI systems:

- Advance verification and validation of the AI system in order to assess and mitigate the risks related to the safety of the AI system.
- Implementation of measures which contribute to the intrinsic safety (reduction of essential risk factors such as kinetic energy of actuators) and functional safety (mitigation of risks by operation of additional control devices such as automatic braking) of AI systems that work with actuators or other devices throughout the development of the AI system to the extent possible in light of the characteristics of the technologies to be adopted.
- Explanations to stakeholders, such as users, about the designers' intentions and reasons for creating AI systems when developing AI systems which are to be used for making judgments regarding the life, body or property of users and third parties (for example, judgments that prioritise the protection of life, body and/or property at the time of an accident of an AI-equipped robot).

**#5 Principle of security** – Developers should pay attention to the security of AI systems.

In addition to respecting international security guidelines, such as the OECD Guidelines for the Security of Information Systems and Networks, developers are encouraged to focus on the following considerations given the possibility that AI systems might change their outputs or programmes as a result of learning or other actions:

- The reliability (that is, whether the operations are performed as intended and not guided by unauthorised third parties) and robustness (that is, tolerance to physical attacks and accidents) of AI systems, in addition to: (a) confidentiality; (b) integrity; and (c) availability of the information that is usually required to ensure the information security of AI systems.
- Advance verification and validation of AI systems in order to assess and control the risks related to the security of the AI systems.
- Implementation of measures to maintain the security of AI systems to the extent possible in light of the characteristics of the technologies to be adopted throughout the process of the development of the AI systems ("*security by design*").

**#6 Principle of privacy** – AI systems should not infringe the privacy of users or third parties.

The privacy referenced in the principle of privacy includes spatial privacy (peace of personal life), information privacy (personal data) and secrecy of communications. Developers should contemplate international guidelines addressing privacy, such as the OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data, as well as the following considerations given the possibility that AI systems might change their outputs or programmes as a result of learning and other actions:

- Evaluation of the risks of privacy infringement and conduct privacy impact assessments in advance.
- Implementation of the measures necessary to avoid infringement of privacy at the time of the utilisation to the extent possible in light of the characteristics of the technologies to be adopted throughout the process of the development of the AI systems ("*privacy by design*").

**#7 Principle of ethics** – Developers should respect human dignity and individual autonomy in the R&D of AI systems.

When developing AI systems that link with the human brain and body, developers are encouraged to respect human dignity and individual autonomy in light of discussions on bioethics, etc. Developers are also encouraged, to the extent possible in light of the characteristics of the technologies to be adopted, to take the measures which are necessary to prevent unfair discrimination resulting from prejudice from being included in the learning data of the AI systems. Furthermore, developers should take precautions to ensure that AI systems do not unduly infringe the values of humanity based on the International Human Rights Law and the International Humanitarian Law.

**#8 Principle of user assistance** – AI systems should support users and provide appropriate opportunities for choice.

In order to support AI system users, developers should consider the following:

- The availability of interfaces which are easy-to-use and provide information that can help users make decisions in a timely and appropriate manner.
- The availability of functions that provide users with opportunities for choice in a timely and appropriate manner (e.g., default settings, easy-to-understand options, feedback, emergency warnings, handling of errors, etc.).
- Implementation of measures to make AI systems easier to use for socially vulnerable people such as universal design.

In addition, developers should endeavour to provide users with appropriate information given the possibility of changes in outputs or programmes as a result of learning or other actions of AI systems.

**#9 Principle of accountability** – Developers should endeavour to be accountable to their stakeholders including AI system users.



Developers are expected to be accountable for the AI systems which they have developed in order to gain the trust of users in AI systems. More specifically, developers are encouraged to provide users with information which helps users choose and utilise AI systems. In addition, in order to improve society's acceptance of AI systems, developers are encouraged to: (a) provide users with explanations and information about the technical characteristics of the AI systems that they have developed; and (b) obtain the active involvement of stakeholders (e.g., user feedback) in order to have a dialogue with diverse stakeholders and learn of various perspectives and views.

Developers are also advised to share information and cooperate with providers who offer services related to the AI systems that they have developed on their own.

#### 4 AI & Data Related Contracts Guidelines

The Ministry of Economy, Trade and Industry (METI) will issue these guidelines in May 2018 or some time thereafter. The author is a member of the working group which is drafting the guidelines. The guidelines consist of a chapter on AI and one on data. The AI chapter analyses legal and business issues and model clauses of AI development contracts and AI service contracts. The guidelines have been subject to public consultation since the end of April 2018 and will be finalised at the end of May 2018.



#### Takashi Nakazaki

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](mailto:takashi.nakazaki@amt-law.com)  
URL: [www.amt-law.com](http://www.amt-law.com)

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 SNS. In addition, he regularly assists the Japanese government in data protection and cyber law areas including "National *Omote-nashi* project" and "AI & Data Contracts Guidelines" and continuously leads IAPP Tokyo 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

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.

# Australia

Trent Taylor



Daniel Clarkin



## Holding Redlich

### 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**).

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

- The *Spam Act 2003* (Cth) (**Spam Act**) regulates commercial email and other types of commercial electronic messages.
- The *Do not Call Register Act 2006* (Cth) (**DNCRA**) sets out restrictions on unsolicited telephone calls.
- Various State and Territory legislation including: the *Invasion of Privacy Act 1971* (Qld); *Information Privacy Act 2009* (Qld); *Privacy and Personal Information Protection Act 1998* (NSW); *Privacy and Data Protection Act 2014* (Vic); *Personal Information Protection Act 2004* (Tas); *Workplace Privacy Act 2011* (ACT); and *Information Privacy Act 2014* (ACT).

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

- The telecommunications sector is also regulated by the *Telecommunications Act 1997* (Cth) and the *Telecommunications (Interception and Access) Act 1979* (which imposes certain data retention obligations on some service providers).
- The health sector in NSW and Victoria is also regulated by the *Health Records and Information Privacy Act 2002* (NSW) and the *Health Records Act 2001* (Vic).

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

The Office of the Australian Information Commissioner (**OAIC**). The Australian Information Commissioner administers the protection of privacy of individuals under the Privacy Act.

The Australian Communications and Media Authority (**ACMA**) enforces the Spam Act and the DNCRA.

The Australian Attorney-General's Department is responsible for providing assistance under the *Telecommunications (Interception and Access) Act 1979*.

State and Territory Privacy, Information and/or Health Information Commissioners administer certain State and Territory privacy legislation.

### 2 Definitions

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

- **“Personal Data”**  
“Personal Information” means 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”**  
This term is not used in the Privacy Act. Processing is covered by two terms in the privacy principles: “use” and “disclosure”.  
“Use” of personal information involves what happens to information within an entity.  
“Disclosure” is the dissemination of the personal information to a separate entity.
- **“Controller”**  
This term is not used in the Privacy Act. The privacy principles regulate the actions of an “APP Entity”. See also the key concept “holds”, as an APP Entity that holds Personal Information is regulated. An APP Entity, subject to certain limitations, covers government agencies, individuals and companies.
- **“Processor”**  
The term “Processor” is not used in the Privacy Act.
- **“Data Subject”**  
The term “Data Subject” is not used in the Privacy Act. Subject to statutory exceptions and exemptions (including for employee records), any individual's personal information that is handled by an APP Entity is subject to the Privacy Act.
- **“Sensitive Personal Data”**  
“Sensitive Information” means personal information about an individual's:  
(a) racial or ethnic origin;  
(b) political opinions;  
(c) membership of a political association;

- (d) religious beliefs or affiliations;
- (e) philosophical beliefs;
- (f) membership of a professional or trade association;
- (g) membership of a trade union;
- (h) sexual orientation or practices; or
- (i) criminal record.

■ **“Data Breach”**

An “eligible data breach” occurs if:

- (a) there is unauthorised access to, unauthorised disclosure of, or loss of, personal information held by an entity; and
- (b) 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.

**“Holds”**

An entity “holds” personal information if the organisation has the right or power to deal with it.

**“De-identified”**

Personal information is de-identified if the information is no longer about an identifiable individual or an individual who is reasonably identifiable.

*See further section 6 of the Privacy Act for general definitions.*

### 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 Privacy Act applies to businesses established in other jurisdictions.

A business established in another jurisdiction will be subject to the Privacy Act if it is an APP Entity or small business operator that has an “Australian Link”.

An “Australian Link” arises (s 5B(2)) if an organisation or operator is:

- (a) an Australian citizen;
- (b) a person whose continued presence in Australia is not subject to a limitation as to time 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.

An organisation or small business operator not described above also has an “Australian Link” (s 5B(3)) if:

- (a) the organisation or operator carries on 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 imposes an obligation on organisations to act openly and transparently when dealing with personal information. This requires the organisations to implement practices, procedures and systems to ensure the organisation is APP compliant. It also requires the organisation to have an up-to-date policy on how to handle personal information.

■ **Lawful basis for processing**

In general, the lawful basis for the use or disclosure of personal information requires an organisation to have the consent of the individual. APP 3 limits collection to information reasonably necessary for functions or activities. An APP Entity may “solicit” personal information if the entity requests another entity to provide the personal information (APP 3.6).

■ **Purpose limitation**

APP 6 covers the use or disclosure of personal information. Subject to certain specific situations, if an individual has provided personal information for a primary purpose then, unless the individual has consented to a separate use or disclosure or the individual would reasonably expect the organisation to use or disclose the information for a secondary purpose related to the primary purpose, the use or disclosure for any other purpose is prohibited.

■ **Data minimisation**

An organisation must not collect personal information (other than sensitive information) unless the information is reasonably necessary for, or directly related to, one or more of the entity’s functions or activities – see further APP 3.

■ **Proportionality**

Under APP 10, an organisation must take reasonable steps to ensure the personal information it uses and discloses is accurate, up to date, complete and relevant.

■ **Retention**

Under APP 11.2, once an organisation no longer needs personal information for the use it was provided for, the entity must take steps to destroy or de-identify the information. There are exceptions relating to certain requirements to hold specific information for a prescribed period, such as a company’s financial records.

■ **Other key principles – please specify**

**Anonymity**

Under APP2, unless there is a requirement by law or it would be impractical, an individual may choose to remain anonymous when dealing with an organisation.

**Access**

APP 12 requires an organisation, on request by an individual, to give an individual access to any personal information the organisation holds on them.

**Notification**

APP 5 requires an organisation to notify an individual of a number of factors at or before the time personal information is collected. If it is not possible at or before the time of collection, they should be notified as soon as practical. This notification must include the purpose of the collection, any other entities the information may be shared with, the privacy policy of the entity, if it is likely to share the information with an overseas recipient and the country of the overseas recipient.

**Direct Marketing**

APP 7 concerns direct marketing. The main principle of direct marketing is that a recipient must have consented to the use of their personal information for direct marketing or provided the information with a reasonable expectation the information would be used for direct marketing. Individuals must have the option to opt-out of any future marketing.

**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 and sets out timeframes within which organisations must respond.
- **Right to rectification of errors**  
APP 13 allows an individual to require an entity to correct the personal information it holds in respect of them.
- **Right to deletion/right to be forgotten**  
This right does not currently exist in Australia. However, an APP Entity must take reasonable steps to destroy or de-identify the personal information it holds once the personal information is no longer needed for any purpose for which the personal information may be used or disclosed under the APPs (APP 11.3).
- **Right to object to processing**  
The use, collection and disclosure of personal information generally require notice and consent. APP 2 provides individuals with the right to deal with organisations anonymously.
- **Right to restrict processing**  
There is no specific right to restrict processing. However, there are restrictions on the collection, solicitation, use and disclosure of personal information, including having regard to the purpose for which the information was supplied – see further APP 3 and APP 6.
- **Right to data portability**  
The right to “data portability” does not exist in Australia. Under APP 12, an individual has a right to request a copy of their personal information from organisations that hold their information.
- **Right to withdraw consent**  
The Privacy Principle Guidelines published by the OAIC indicate an individual may withdraw their consent at any time. If an individual withdraws consent, the organisation may no longer rely on the past consent for any future use or disclosure of personal information.
- **Right to object to marketing**  
Under APP 7, an organisation must cease direct marketing, using or disclosing personal information for direct marketing if they receive a request from an individual to cease.
- **Right to complain to the relevant data protection authority(ies)**  
Individuals have a right to complain to the Information Commissioner if they believe there has been an interference with their privacy. The Information Commissioner then has a number of powers to investigate and resolve the complaint.
- *Other key rights – please specify*  
**Right to anonymity and pseudonymity**  
Under APP 2, individuals must have right of not identifying themselves or using a pseudonym unless it is impractical for an organisation to deal with them in that way.

**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, other than the mandatory data breach notification requirements in respect of eligible data breaches, as described further below. Otherwise, there is no legal obligation on businesses to generally register with or notify the Office of the Australian Information Commissioner in respect of 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)?**

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 is not mandatory. APP 1 does require an organisation to implement practices, procedures and systems to ensure the entity is APP compliant. Appointing a privacy officer is one step an organisation can take to establish compliance with the privacy principles.

**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 to 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?**

There are no statutory restrictions or obligations in relation to the appointment of data protection officers. However, the OAIC recommends an organisation appoint key roles and responsibilities for privacy management, including a senior member of staff with overall accountability for privacy and staff responsible for managing privacy, including a key privacy officer.

**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?**

The OAIC recommends that privacy officers are responsible for handling internal and external privacy enquiries, complaints, and access and correction requests.

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

No, such action does not need to take place.

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

No, the data protection officer does not need to be named in such documents.

**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?**

This is not applicable. Best practice is to ensure that a processor complies with any privacy laws applicable to the organisation. Further, where there is now a requirement for an organisation to report eligible data breaches, an organisation should include a contractual obligation on processors to promptly inform the organisation in respect of any identified eligible data breaches in respect of personal information transmitted to or generated from or in connection with that personal information by that 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.)?**

In addition to the above matters, best practice is for the agreement to be in writing.

**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?)**

APP 7 prohibits an organisation from using or disclosing an individual's personal information for direct marketing unless:

1. the organisation collected the information, the individual would reasonably expect the information to be used for this purpose and the individual has a method of opting out; and
2. the individual has consented to the use or disclosure for direct marketing (unless it is impractical to obtain the consent) and each communication draws attention to the ability of the individual to opt-out.

The Spam Act also regulates the sending of unsolicited commercial emails.

**9.2 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 DNCRA regulates telemarketing.

If a number is listed in the Do Not Call Register, then, subject to obtaining consent in accordance with the DNCRA, an organisation is generally prohibited from contacting the number.

The Spam Act regulates text messages, multimedia messages, instant messaging and email.

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

The Spam Act and the DNCRA extend to things done outside Australia where there is an “Australian Link”.

Under the Spam Act, an “Australian Link” (s 7) arises if:

- (a) the message originates in Australia;
- (b) the individual or organisation who sent the message, or authorised the sending of the message, is:
  - (i) an individual who is physically present in Australia when the message is sent; or
  - (ii) an organisation whose central management and control is in Australia when the message is sent;
- (c) the computer, server or device that is used to access the message is located in Australia;
- (d) the relevant electronic account-holder is:
  - (i) an individual who is physically present in Australia when the message is accessed; or
  - (ii) an organisation that carries on business or activities in Australia when the message is accessed; or
- (e) if the message cannot be delivered because the relevant electronic address does not exist – assuming that the electronic address existed, it is reasonably likely that the message would have been accessed using a computer, server or device located in Australia.

The DNCRA applies to a telemarketing call or a marketing fax sent to an “Australian number”.

If the business has an “Australian Link”, the Privacy Act will apply and the Commissioner will deal with complaints about overseas acts.

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

Yes, the OAIC regularly investigates and enforces alleged breaches of the Privacy Act, and publishes outcomes on its website.

The ACMA is active in the enforcement of breaches of the Spam Act, assisted by a high number of complaints. The ACMA has the authority to issue infringement notices and commence enforcement proceedings against organisations that breach the Spam Act or the DNCRA.

### **9.5 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 restriction on purchasing a marketing list from a third party. However, prior to sending direct marketing to the recipients on the list, an organisation must ensure the recipients have consented to receiving the direct marketing. It is the responsibility of the organisation sending the marketing to show consent has been obtained. It is best practice to obtain written details of how the provider obtained the contact details and under what terms and conditions.

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

The maximum penalty for an initial offence under the Spam Act is \$84,000 per day for an individual and \$420,000 per day for a body corporate. For a repeat offence, the maximum rises to \$420,000 per day for an individual and \$2.1 million per day for a body corporate. The court may also order compensation if the recipient has suffered loss due to the messages.

Under the DNCRA fines may be up to \$2.1 million.

Under the Privacy Act a fine of up to \$2.1 million may also apply.

## **10 Cookies**

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

There is no specific legislation governing the use of cookies. The privacy principles apply to cookies where a user is reasonably identifiable. In those situations, organisations are obliged to comply with them.

To comply with APP 2, websites should make it possible for users to block cookies which collect information that can be linked to an identified individual while continuing to make the site functional for these people.

### **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?**

As at 17 April 2018, the ACMA and the OAIC have not reported any enforcement actions in relation to cookies.

### **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.**

Under APP 8, before an organisation discloses personal information to an entity outside of Australia, the organisation must take reasonable steps to ensure the recipient does not breach the APPs, unless:

- (a) the recipient is subject to laws similar to the APPs and there are mechanisms for the affected person to take action or enforce the laws; or
- (b) the individual provides their consent to the disclosure.

There are restrictions on the disclosure of certain types of information. Part IIIA of the Privacy Act includes some restrictions on sending certain credit reporting overseas. The Australian Government's My Health Record framework limits the disclosure of health records overseas. Some State legislation limits disclosure of some health information into separate jurisdictions.

**11.2 Please describe the mechanisms companies 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 are generally expected to enter into enforceable contractual arrangements with overseas recipients (and require the overseas recipient to enter into similar contracts with any third parties) to handle the personal information in accordance 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 for the transfer of personal data.

## 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.)?**

Organisations have an obligation to provide notice to an individual if it collects their personal data. Providing notice would not be required if the information received is solely related to employment. If a third party is used to run the hotline, the employee records exemption will not apply as the party collecting the information will not be the employer. How an employer handles the information will depend on the information provided.

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

Anonymous reporting is not prohibited under the Privacy Act. If a party is to be protected by whistle-blower protections, they must identify themselves by name when making disclosure to the relevant person or authority to qualify for the whistle-blower protections in the Corporations Act.

## 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 requires notice to individuals subject to

surveillance. There is no requirement to register or seek approval. Specific rules vary depending upon the State or Territory.

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

The States each have their own legislation regulating the use of surveillance devices. Generally, CCTV is prohibited in respect to recording private activities.

## 14 Employee Monitoring

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

Employee surveillance requirements differ between the jurisdictions. CCTV surveillance in the workplace is permitted (subject to notice requirements in New South Wales (NSW) and the Australian Capital Territory (ACT)). In NSW and the ACT, employees must be given notice of the surveillance to be carried out.

In general terms, employers can log all employee use of company email and computer systems, including the email addresses to which messages are sent, websites visited, times of access and transmissions. Employers should develop an email and computer usage policy and communicate this with their employees. Employers can also gain access to the content of email messages. Employers do not have to seek the consent of their employees to be able to monitor and access such communications and transactions lawfully, but the way in which they conduct surveillance is subject to specific legislative requirements.

With regards to employee drug testing, provided such testing is conducted for the purposes of obtaining information about the employee's employment, the Privacy Act will not apply.

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

In NSW and the ACT, employers are required to provide 14 days' notice detailing the surveillance.

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

This is not addressed in the privacy legislation.

## 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.)?**

There is a general requirement under APP 11 to take reasonable steps to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

Any entity that holds personal information is responsible for ensuring the security of the information.

**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) expects voluntary breach reporting.**

The Notifiable Data Breach Scheme commenced on 22 February 2018. This requires an organisation to report to the OAIC and any individuals affected if they reasonably believe an eligible data breach has occurred. Eligible data breaches are those that could result in serious harm to the affected individuals.

If an organisation suspects a breach has occurred, they generally have 30 days to investigate the breach. If during the investigation, the organisation believes the breach has occurred, they must notify the Information Commissioner of:

- (a) the identity and contact details of the organisation;
- (b) a description of the breach;
- (c) the type of information concerned; and
- (d) recommendations about the steps that should be taken, as soon as practical, and then inform the affected party.

**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) expects voluntary breach reporting.**

Yes, as above.

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

Penalties are imposed by the Information Commissioner. They may range from a personal apology to a fine of \$2.1 million.

## 16 Enforcement and Sanctions

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

Investigatory Powers	Civil/Administrative Sanction	Criminal Sanction
Investigating complaints by individuals of alleged privacy interferences	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) Seek an injunction including before, during or after an investigation or the exercise of another regulatory power (s 98) Apply to the court for a civil penalty order for a breach of a civil penalty provision (s 80W) Fines of up to \$2.1 million may be imposed under the Privacy Act	Not applicable
Investigating possible breaches where the commissioner considers it desirable that an act be investigated	As above, as well as report to the Minister in certain circumstances following a Commissioner-initiated investigation (s 30)	Not applicable
Attempt to conciliate a complaint	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)	Not applicable
Require information or documents to be produced, or a person to attend before the Commissioner to answer questions under oath	Not applicable	Failure to comply with the lawful requirements of the Commissioner may result in a fine or possible imprisonment

**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?**

There has been no such ban to date. However, the OAIC may make a public interest declaration noting that certain actions that would normally be a breach of the privacy principles shall not be regarded as being a breach due to the public interest of the actions. Organisations may make an application to the Commissioner to obtain a declaration.



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

After receiving a complaint from an affected party, the Information Commissioner will often seek to conciliate complaints between the parties and help them come to an agreement. The Information Commissioner also investigates potential breaches and has power to make determinations and accept enforceable undertakings. In serious cases the Information Commissioner has the power to seek civil penalties to ensure compliance with the Privacy Act.

A recent determination was made against The Westin Sydney for recording an individual's telephone conversation without their knowledge. The determination required The Westin Sydney to issue an apology and pay the complainant \$1,500.

In July 2017, after investigating the Australian Red Cross Blood Service, the Information Commissioner took an enforceable undertaking from them to conduct a review of their policies and the Red Cross had to agree that the Information Commissioner may inform the media of the reasons for obtaining the undertaking.

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

In 2017, the OAIC investigated Avid Life Media Inc (ALM), the company that operates the adult dating website Ashley Madison. Following the publication of user details, the OAIC worked with the Privacy Commissioner of Canada to investigate the operation of ALM. Following the investigation, the OAIC provided a number of recommendations and accepted an enforceable undertaking from ALM in relation to the recommendations.

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

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

Requests for disclosure of personal information are handled under APP 6 (use and disclosure) and APP 8 (cross-border disclosure). This may require the organisation to obtain the individual's consent.

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

The only guidance issued is the general cross-border disclosure guidance.

## 18 Trends and Developments

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

The OAIC continues to monitor possible breaches and make determinations. As recently as 23 March 2018, the OAIC issued a determination against Cbus requiring them to apologise for disclosing personal information to an external organisation for a secondary purpose without consent.

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

Mandatory data breach notification requirements were introduced in February 2018. The scheme is intended to ensure individuals are notified as early as possible that their data may not be secure.

On 5 April 2018, the OAIC opened a formal investigation into Facebook following confirmation from Facebook that information of over 300,000 Australian users may have been acquired and used without authorisation.

**Trent Taylor**

Holding Redlich  
Level 1  
300 Queen Street  
Brisbane, Queensland, 4000  
Australia

*Tel:* +61 7 3135 0668  
*Email:* [trent.taylor@holdingredlich.com](mailto:trent.taylor@holdingredlich.com)  
*URL:* [www.holdingredlich.com](http://www.holdingredlich.com)

Trent is a Brisbane-based Partner in Holding Redlich's Corporate and Commercial Group.

Trent specialises in technology and data protection.

Trent's clients include major corporations operating in the property, technology, manufacturing, distribution and franchising industries.

Trent has handled a variety of ICT projects for both suppliers and customers.

Trent regularly advises in connection with project work and regulatory compliance matters.

**Daniel Clarkin**

Holding Redlich  
Level 1  
300 Queen Street  
Brisbane, Queensland, 4000  
Australia

*Tel:* +61 7 3135 0693  
*Email:* [daniel.clarkin@holdingredlich.com](mailto:daniel.clarkin@holdingredlich.com)  
*URL:* [www.holdingredlich.com](http://www.holdingredlich.com)

Daniel is a Brisbane-based Solicitor in Holding Redlich's Corporate and Commercial Group.

Daniel works with clients in the information technology sector, including licensors and resellers of software and data. He has advised a number of clients, including online businesses in connection with data collection and protection.

Key clients include operators in the property, development, technology and franchising industries.

Daniel uses his training in the defence forces in his legal career and is adept at meeting deadlines and managing projects.

**HOLDING REDLICH**

Holding Redlich clients do not just receive legal advice. They receive advice they can use, tailored to their needs, underpinned by the very best legal thinking and expert industry knowledge. At Holding Redlich, we tackle projects with a commitment to excellence and business focus. An understanding of our clients' commercial issues coupled with impeccable application of the law brings results. Above all else, we understand that our job is to look after our clients and their best interests. Integrity and trust are at the core of our relationships with them.

Holding Redlich is a national Australian commercial law firm with offices in Sydney, Melbourne, Brisbane and Cairns. We are one of Australia's leading law firms with the resources and expertise of more than 350 staff, including over 150 lawyers, more than 50 of whom are partners. Our lawyers have extensive experience in advising clients on the impact of the Privacy Act and ancillary legislation.

# Austria

Herbst Kinsky Rechtsanwälte GmbH

Dr. Sonja Hebenstreit



Dr. Isabel Funk-Leisch



## 1 Relevant Legislation and Competent Authorities

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

From 25 May 2018, the principal data protection legislation in the EU will be Regulation (EU) 2016/679 (the “General Data Protection Regulation” or “GDPR”). The GDPR repeals Directive 95/46/EC (the “Data Protection Directive”) and leads to increased (though not total) harmonisation of data protection law across the EU Member States.

The Data Protection Act Adaptation Act 2018 (“*Datenschutzgesetz-Anpassungsgesetz 2018*”) Federal Law Gazette (“*Bundesgesetzblatt*” – “BGBl”) I Nr. 120/2017 amends the current Data Protection Act 2000 (“*Datenschutzgesetz 2000*”) in accordance with the GDPR and will enter into force on 25 May 2018 as the Austrian Data Protection Act (“*Datenschutzgesetz*”, hereinafter “DSG”). Furthermore, Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA is implemented into Austrian law by the Data Protection Act Adaptation Act 2018.

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

Data protection is impacted by labour law. The DSG 2000 did not contain a systematic regulation of data protection in the context of employment, but the principal legislation on data protection regarding labour law is the Works Council Constitution Act (*Arbeitsverfassungsgesetz* – hereinafter referred to as “ArbVG”); in particular, sections 96 and 96a ArbVG. For certain data processing activities, the consent of the works council is mandatory (please see questions in section 14).

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

Other sector-specific legislation can, e.g., be found in the Telecommunications Act 2003 which contains the implementation of the EU Data Protection Directive on Electronic Communications (e.g., provisions regarding commercial electronic communication, cookies, etc.), as well as in the Banking Act (banking secrecy).

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

The “*Datenschutzbehörde*” (hereinafter “DSB”) is the national independent supervisory authority in Austria (see section 18 para 1 DSG).

Another institution is the Data Protection Council (“*Datenschutzrat*”), which is responsible for advising the Federal Government and the State Governments on requests concerning data protection law (section 14 *et seq.* DSG).

Until 24 May 2018, Austrian data protection law requires the registration of data applications with the DSB. This data processing register (“*Datenverarbeitungsregister*”) will be continued for archiving purposes until 31 December 2019.

## 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**” (or “Special Categories Of 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 interest 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 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 in Austria, if the data subjects lives in Austria or the alleged infringement occurred in Austria.

■ **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?

Until 24 May 2018, every processing activity required prior notification to the DSB (and in some cases even prior approval), unless a legal exception applied. As from 25 May 2018, the DSG no longer contains any such general notification obligations.

However, the DSG provides in its sections 7 and 8 for specific requirements for prior approval of the DSB (a) in the context of data processing in the public interest for the purposes of archiving, scientific or historical research or statistics, and (b) in the context of processing address data of data subjects for purposes of an important public interest regarding the notification or interview of that subjects.

The data processing register will be continued for archiving purposes until 31 December 2019.

The DSB has stated in its official guideline to the GDPR that all documentation to be provided to the DSB in the course of an (examination) proceeding (e.g., processing register, data protection impact assessment (“DPIA”)) needs to be in German.

### 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 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)?

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)?

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)?

Please see question 6.1 above.

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

Please see question 6.1 above.

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

Please see question 6.1 above.

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

Please see question 6.1 above.

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

Please see question 6.1 above.

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

Please see question 6.1 above.

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

Please see question 6.1 above.

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

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.**

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.

Austria has not made use of the possibility offered in Article 37 para 4 GDPR and has not provided for any further mandatory Data Protection Officer designation requirement.

**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. In particular, it is subject to an administrative fine of the higher of up to 10 Mio EUR or 2% of the annual turnover of the respective controller according to Article 83 para 4 GDPR.

**7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect to 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.

In accordance with section 5 DSG, the Data Protection Officer is bound by secrecy towards in particular the identity of any persons who have contacted the Data Protection Officer. In case the respective data subject has a privilege to refuse to give legal evidence, and has made use of such privilege, the Data Protection Officer may not provide any information regarding the respective data.

**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 DPIAs 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 ("WP29") recommends 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 a written 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).

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 Data Protection Officer; (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 section 107 para 2 Austrian Telecommunications Act ("*Telekommunikationsgesetz 2003*", containing the implementation of Directive 2002/58 EC, as amended; hereinafter "TKG"), the sending of electronic mail – including SMS messages – without the recipient's prior consent shall not be permitted if the sending takes place for purposes of direct marketing or is addressed to more than 50 recipients. Such prior consent shall not be required, if:

- contact details for the communication were obtained in the context of a sale or a service to the recipient;
- the communication is transmitted for the purpose of direct marketing of his own similar products or services; and
- the recipient clearly and distinctly has been given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details and the recipient did not register in the "Robinson List" (section 7 Austrian E-Commerce Act).

For reasons of clarity, it is advisable to get prior consent of the recipient for any email or SMS marketing activities.

### 9.2 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 section 107 para 1 TKG, marketing by telephone, including facsimile transmissions for marketing purposes, shall not be permitted without the prior consent of the subscriber. Please note that prior consent may not be received in the course of the first call, but needs to be given before. For marketing by post, no restrictions (as applicable for calls or emails) apply.

### 9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

If unlawful direct marketing actions have not been committed in Austria, they shall be considered as having been committed in the place where the call reaches the subscriber's line. As a result, this means that any direct marketing action is judged according to the aforementioned rules when the message/call was received in Austria. However, it is often not possible for the authority to prosecute legal violations abroad.

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

The competent authority for the enforcement of section 107 TKG is the Telecommunications Authority ("*Fernmeldebehörde*"); the data protection authority is not responsible for the enforcement of such violations. The authority mainly becomes active when somebody makes a complaint.

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

Undertakings holding a licence under section 151 Austrian Trade Act ("*Gewerbeordnung*") are entitled to collect data from publicly available sources (and to add classifications for specific marketing purposes) for the preparation and execution of marketing purposes for third parties and are entitled to sell such lists to third parties. The purchase of such lists will therefore be admissible. However, when using purchased marketing lists from third parties for the purpose of sending any electronic communication, it needs to be safeguarded that the recipient of the advertising has indeed given consent for electronic direct marketing.

### 9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

The infringement of section 107 para 2 TKG (emails/SMS for marketing purposes without consent) constitutes an administrative offence which is punishable by a fine of up to EUR 37,000.

The infringement of section 107 para 1 (calls/fax for marketing purposes without consent) TKG constitutes an administrative offence which is punishable by a fine of up to EUR 58,000.

## 10 Cookies

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

Section 96 para 3 TKG 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 Directive 95/46/EC and, from 25 May 2018, the GDPR). For consent to be valid, it must be informed, specific, freely given and must constitute a real 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, which means that it must be essential to fulfil their request.

### 10.2 The EU Commission intends to pass a new ePrivacy Regulation that will replace the respective national legislation in the EU Member States. The regulation is planned to come into force May 25, 2018 and will provide amended requirements for the usage of cookies. Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

The WP29 published a Working Document 02/2013 (WP 208) providing guidance on obtaining consent for cookies. Following WP29, the consent to the use of cookies containing personal data has to be explicit opt-in consent. The opinion of WP29 is not mandatory but it is usually used by the relevant authorities to determine the content of data protection legislation; in this case, section 96 para 3 TKG and the necessary consent.

However, section 93 para 3 TKG 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?

We are not aware of any publicly known enforcement action in this respect.

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

An infringement of section 96 para 3 TKG constitutes an administrative offence which is punishable by a fine of up to EUR 37,000.

## 11 Restrictions on International Data Transfers

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

Data transfers to 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) or the business has implemented one of the required safeguards as specified by the GDPR.

### 11.2 Please describe the mechanisms companies 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.

Transfer of personal data to the US is also possible if the data importer has signed up to the EU-US Privacy Shield Framework, which was designed by the US Department of Commerce and the EU Commission to provide businesses in the EU and the US with a mechanism to comply with data protection requirement when transferring personal data from the EU to the US.

### 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.



## 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, 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. The WP29 recommends 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.

Article 10 GDPR requires that the processing of personal data relating to criminal convictions and offences shall only be carried out under the control of official authority or when the processing is authorised by EU or a Member State's law. In Austria, this would currently be given for whistle-blower hotlines of financial institutions according to section 99g Banking Act ("*Bankwesengesetz*").

### 12.2 Is anonymous reporting prohibited, or 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, the WP29 considers 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)?

The use of CCTV is allowed if made in accordance with sections 12, 13 DSG. In such case, no DPIA must be undertaken in line with Article 35 para 10 GDPR. Sections 12 and 13 DSG have been enacted in accordance with Article 6 para 2 and 3, Article 23 and chapter IX GDPR and following the experiences made with the rules on CCTV that were contained in the DSG 2000.

In principle, CCTV is allowed if:

- it is required in the vital interest of a person;
- the data subject has consented to the use of its data;
- it is allowed by specific legal provisions; or
- in case of preponderant legal interests of the controller or a third person, provided that the processing is proportionate.

Section 12 para 3 DSG 2000 specifies that preponderant legal interests are given in case the CCTV is made for purposes of:

- the precautionary protection of persons or things on private property that is used only by the controller;
- the precautionary protection of persons or things on publicly accessible property being under the domestic authority of the controller, in case violations have already been happened in the past or there is a specific potential danger; or
- a private documentation interest in case the CCTV is neither directed to capture uninvolved persons, in a way allowing their identification nor to capture objects which would indirectly allow the identification of such persons.

CCTV in principle needs to be specifically marked by a sign which identifies the respective controller (section 13 para 4 DSG).

The DSB has stated in its draft White List for the DPIA that specific CCTV processing (as defined in the White List) does not require a DPIA.

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

According to section 12 para 4 DSG, CCTV is not permitted for the purpose of (i) control of employees in the workplace (please see question 14.1 below), (ii) automation-supported comparison of personal data obtained by means of CCTV with other personal data, and (iii) the evaluation of personal data obtained by means of CCTV on the basis of special categories of personal data (Article 9 GDPR) as a selection criterion.

Section 13 para 3 provides that any recordings need to be deleted if they are no longer required for the purpose for which they were collected, unless another legal obligation applies. In any case, the storing of recordings exceeding 72 hours needs to be proportionate and needs to be separately documented and justified.

## 14 Employee Monitoring

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

Section 12 para 4 number 1 DSG provides that CCTV is prohibited at locations that are deemed to be part of the most personal area of

the data subject's life (e.g., their homes in general and also changing rooms, bathrooms, etc.) without explicit consent.

Furthermore, CCTV for the purpose of control of employees in the workplace (efficiency control) is expressly prohibited (section 12 para 4 number 2 DSG).

This provision does not generally prevent the surveillance of workplaces (e.g., the surveillance of dangerous machines in order to protect the employees or the surveillance of, e.g., the counter hall of a bank), as long as the purpose is not efficiency control or employee monitoring as such. In most cases of video surveillance of a workplace, the works council will need to give its consent to such surveillance. Furthermore, please refer to the answers to section 13 above.

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

Pursuant to section 13 para 4 DSG, CCTV must be marked appropriately.

If a works council is established in the respective entity, an agreement needs to be concluded with the works council. Individual consent of the employee does not suffice in this case. In cases where no works council is established, each employee needs to provide its consent to the respective video surveillance of its workplace (if such is not already prohibited by section 12 para 4 number 2 DSG).

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

Please see 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 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 EUR 20 million or 4% of worldwide turnover.

## 16 Enforcement and Sanctions

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

Investigatory Powers	Civil/Administrative Sanction	Criminal Sanction
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.	N/A

Investigatory Powers	Civil/Administrative Sanction	Criminal Sanction
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). Please note that even attempted data breaches may be punished; and further, any data carrier or programmes, as well as picture transmitting or recording devices, may be confiscated if they are linked to an offence (section 62 DSG).	The unlawful use of data with the intention to enrich itself or a third party or to cause damage to third parties is a criminal offence punishable by imprisonment for up to one year or a fine of up to 720 daily rates (section 63 DSG). The Competent Authority is the Criminal (District) Court.
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.	N/A
Imposition of Administrative Fines for Infringements of Specified GDPR Provisions	The GDPR provides for administrative fines which can be EUR 20 million or up to 4% of the business' worldwide annual turnover of the preceding financial year. The DSG contains further administrative fines – subsidiary to the GDPR fines – of up to EUR 50,000.	N/A
Non-Compliance With a Data Protection Authority	The GDPR provides for administrative fines which will be EUR 20 million or up to 4% of the business' worldwide annual turnover of the preceding financial year, whichever is higher.	N/A

#### 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 – in Austria the DSB – to impose a temporary or definitive limitation including a ban on processing. Such ban can be imposed by the DSB by rendering a decision (“Bescheid”); no court order is required.

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

Because the GDPR has not come into force (at the time of writing these replies), the data protection authority's approach to exercising those powers may not be described yet.

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

Please see question 16.3 above.

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

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

Austrian law does not contain an equivalent to discovery or e-discovery as known in US law. Foreign e-discovery requests will generally collide with data protection law, as the normal rules will apply as to whether it is permitted to transfer data a) to a third person, and b) to a country outside the EEA which does not provide for adequate data protection.

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

The DSB has so far not issued any guidance in this respect.

### 18 Trends and Developments

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

In 2017, one of DSB's focuses was on public hospitals. The reviews showed that the healthcare providers largely complied with the provisions of the data protection laws; however, the DSB has issued recommendations to the hospitals.

Furthermore, DSB has provided guidance regarding the GDPR throughout 2017 and continues this activity in 2018. One major activity of the DSB this year will most likely consist of measures in the context of the GDPR getting into force on 25 May 2018.

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

Austria has already enacted an “implementation act” to the GDPR. Further national laws in the context of the GDPR (including a law slightly amending the Data Protection Adaptation Act) are in the legislative process and will probably be published in the Federal Gazette in May 2018.

The amended section 11 DSG (not yet in force) explicitly states that the DSB shall, in line with Article 58 GDPR, in case of a first infringement of the GDPR, use its corrective powers in particular by issuing warnings.

The most important topic for the DSB is the GDPR and the changed legal framework. The DSB has published a guidance document in 2018 (available only in German) in which certain aspects of the GDPR are commented. In particular, the DSB has published a draft regulation regarding processing activities not requiring a DPIA (“white list”). A (draft) “black list” has not been issued so far.

**Dr. Sonja Hebenstreit**

Herbst Kinsky Rechtsanwälte GmbH  
Dr. Karl Lueger-Platz 5  
A-1010 Vienna  
Austria

*Tel:* +43 1 904 2180 161  
*Fax:* +43 1 904 2180 210  
*Email:* sonja.hebenstreit@herbstkinsky.at  
*URL:* www.herbstkinsky.at

Dr. Sonja Hebenstreit is a partner of Herbst Kinsky Rechtsanwälte GmbH, which she joined in 2005. She specialises in the fields of intellectual and industrial property law, unfair competition, pharmaceutical law, antitrust and competition law, as well as in data protection law.

**Education and Career:** *Mag. iur.* (Vienna 1997); *Dr. iur.* (Vienna 2001); internship with the European Commission (Brussels 1998); trainee at British Telecommunications Group Legal Services (Brussels 1999); researcher at the University of Münster, ITM/Civil Law Department (1999–2000); law practice with Hausmaninger Herbst Attorneys at Law (2000–2005); and Herbst Kinsky Rechtsanwälte GmbH since 2005. Admitted to the Austrian Bar (Vienna 2003).

**Languages:** German; English; and French.

**Dr. Isabel Funk-Leisch**

Herbst Kinsky Rechtsanwälte GmbH  
Dr. Karl Lueger-Platz 5  
A-1010 Vienna  
Austria

*Tel:* +43 1 904 2180 152  
*Fax:* +43 1 904 2180 210  
*Email:* isabel.funk@herbstkinsky.at  
*URL:* www.herbstkinsky.at

Dr. Isabel Funk-Leisch joined Herbst Kinsky Rechtsanwälte GmbH in 2008. She specialises in commercial law, public law, pharmaceutical law, data protection law as well as in the field of insurance intermediation.

**Education and Career:** *Mag. iur.* (Vienna 2004); *Dr. iur.* (Vienna 2008); law practice as an associate at a law firm in Vienna specialised in the field of commercial law; and associate at Herbst Kinsky Rechtsanwälte GmbH in 2008. Admitted to the Austrian Bar (Vienna 2010).

**Languages:** German; English; and French.

## HERBST KINSKY

### RECHTSANWÄLTE GMBH

**The Firm**

Since its establishment in 2005, Herbst Kinsky has become one of Austria's leading commercial law firms. Its specialised and highly committed lawyers combine many years of experience gained abroad and in reputable Austrian law firms. The firm's practice covers a full range of services in all areas of commercial, corporate, civil and public law, including banking, insurance and capital markets, corporate and M&A, IP, IT and life sciences, merger control, antitrust and competition, data protection, real estate, dispute resolution and arbitration.

**Our Clients**

The firm's clients range from large international privately-held and publicly-listed companies, banks, insurance companies and private equity investors to small and mid-size business entities. Clients cut across many different industries, including energy, information technology, financial institutions, insurance, engineering, construction, pharmaceuticals and healthcare.



# Belgium

Lydian

Bastiaan Bruyndonckx



Olivia Santantonio



## 1 Relevant Legislation and Competent Authorities

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

From 25 May 2018, the principal data protection legislation in the EU will be Regulation (EU) 2016/679 (the “**General Data Protection Regulation**” or “**GDPR**”). The GDPR repeals Directive 95/46/EC (the “**Data Protection Directive**”) and leads 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 that would harmonise the applicable rules across the EU.

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 will carry the name “**Data Protection Authority**”.

In addition, the Belgian Parliament will adopt secondary legislation pursuant to the GDPR. A so-called “**GDPR Framework Act**” (the “**GDPR Framework Act**”) is currently under preparation but has not yet been adopted.

### 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.

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

Currently, the authority responsible for data protection is the Commission for the Protection of Privacy. As of 25 May 2018, the Commission for the Protection of Privacy will carry the name “**Data Protection Authority**” and will have the powers which need to be conferred to the supervisory authority pursuant to the GDPR.

## 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.
- “**Special Categories of Data**” or “**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.
- **“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 a 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 interest 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 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**

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 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 direct 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, if the data subjects lives in Belgium or the alleged infringement occurred in Belgium.

■ **Right to 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. The obligation to notify the Commission for the Protection of Privacy of any wholly or partially automated processing of personal data, which existed prior to the entry into force of the GDPR, will be abolished as of the entry into force of the GDPR on 25 May 2018. The public register kept by the Commission for the Protection of Privacy will be closed for consultation as of 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 to a country not offering adequate protection of personal data and that are based upon bespoke contractual safeguards rather than Standard Contractual Clauses approved by the EU Commission.

#### 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; or (ii) large-scale processing of sensitive personal data.

So far, the Belgian legislator has not adopted secondary legislation which 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.

#### 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 the wide range of penalties available under the GDPR, including administrative fines. It is likely that, pursuant to the Belgian GDPR Framework Act, the failure to appoint a Data Protection Officer where such appointment is mandatory, will also be criminally sanctioned.

#### 7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect to 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 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?

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 ("DPIAs") 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") recommends 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 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 or other legal act in writing, including in 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 carrying out DPIAs and obtaining approval from the Data Protection Authority, where required; (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 the 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](mailto: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 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 “Robinson List”) exists and companies 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 the companies that are member of the Belgian Direct Marketing Association (“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).

---

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

---

Yes, they do.

---

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

---

Under the legislation in effect prior to the GDPR, any individual could file a complaint with the Commission for the Protection of Privacy in order to exercise his/her rights of information and objection. The Commission for the Protection of Privacy acted primarily as a mediator in the conflict between the controller and the individual. If no agreement could be found, the Commission for the Protection of Privacy issued an advice on the matter, including recommendations for the controller. Under the GDPR, the Data Protection Authority will have the right to carry out investigations and enforce the GDPR, including by imposing administrative sanctions.

It should be noted that, 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.

---

**9.5 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.

---

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

---

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.



## 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 Directive 95/46/EC and, as of 25 May 2018, the GDPR). For consent to be valid, it must be informed, specific, freely given and must constitute a real 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 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.

### 10.2 The EU Commission intends to pass a new ePrivacy Regulation that will replace the respective national legislation in the EU Member States. The regulation is planned to come into force May 25, 2018 and will provide amended requirements for the usage of cookies. 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, such as, 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 ("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 (until 25 May 2018, the Commission for the Protection of Privacy). In 2017, the Commission for the Protection of Privacy has taken 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 has been condemned by the Brussels Court of First

Instance for having tracked an internet user without them neither knowing nor consenting. The court has issued a fine of EUR 250,000 per day with a maximum fine of EUR 100,000,000. Other than the high-profile Facebook case mentioned above, we are not aware of other enforcement actions taken by the Commission for the Protection of Privacy specifically in relation to cookies.

### 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 criminal fines applicable for breaches of the data protection laws. Under the current legislation based upon the Data Protection Directive, a breach of the data protection legislation can give rise to criminal fines of up to EUR 100,000. This amount is to be multiplied by eight in accordance with the law on criminal surcharges.

## 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) or the business has implemented one of the required safeguards as specified by the GDPR.

### 11.2 Please describe the mechanisms companies 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.

Transfer of personal data to the US is also possible if the data importer has signed up to the EU-US Privacy Shield Framework, which was designed by the US Department of Commerce and the EU Commission to provide businesses in the EU and the US with a mechanism to comply with data protection requirements when transferring personal data from the EU to the US.

---

**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.

## 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. The WP29 recommends 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 has 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.

---

**12.2 Is anonymous reporting prohibited, or 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, the WP29 considers 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 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.

Moreover, according to current Belgian legislation on surveillance cameras, installing CCTV in public areas is only permitted after a positive advice of the communal or city council. In addition, when installing CCTV in public areas, the controller must inform the chief of local 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 at 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 at 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 at the workplace) and Collective Bargaining Agreement N° 81 (on the monitoring of electronic communications at the workplace):

- the employer may monitor the worked hours 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 at the workplace is permitted to the extent the data protection laws and the 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 at the workplace is permitted to the extent the data protection laws and the 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 at the workplace and Collective Bargaining Agreement N° 81 concerning the protection of workers' private lives in respect of the monitoring of electronic communications at 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 at the workplace and the monitoring of electronic communications at 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 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).**

Investigatory Powers	Civil/Administrative Sanction	Criminal Sanction
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.	N/A

Investigatory Powers	Civil/Administrative Sanction	Criminal Sanction
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).	N/A
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.	N/A
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' worldwide annual turnover of the preceding financial year.	N/A
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' worldwide annual turnover of the preceding financial year, whichever is higher.	N/A

**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 7 December 2017 on the establishment of the Data Protection Authority, the inspection chamber of the Data Protection Authority can order by way of 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 dispute chamber can order that 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.**

It is too soon to know the Data Protection Authority's approach to exercising its powers under the GDPR. Under the current legislation



based upon the Data Protection Directive, the Commission for the Protection of Privacy does not have the power to issue a ban on a particular processing activity. However, it may 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 has 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.

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

Under current legislation based upon the Data Protection Directive, the Commission for the Protection of Privacy does indeed exercise its powers against businesses established in other jurisdictions. On 16 February 2018, the Brussels Court of First Instance has condemned Facebook, including Facebook Ireland Limited and Facebook Inc., for having tracked internet users without their knowledge or consent. The court has 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.

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

#### **17.1 How do companies 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 Commission for the Protection of Privacy has not issued any specific opinions on the subject, but 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 Commission for the Protection of Privacy is determined to act against large international companies that do not comply with the applicable data protection legislation. This is illustrated, amongst others, by the investigations that the Commission for the Protection of Privacy has carried out into the activities of Facebook. Already in 2015, the Commission for the Protection of Privacy issued a recommendation and a letter of default to Facebook for violations of the restrictions on cookies. As a result of that, Facebook was convicted for the first time in 2015, after which the Court of Appeals ruled in favour of Facebook on 16 June 2016. However, the Commission for the Protection of Privacy started new proceedings against Facebook in 2017 and obtained a favourable decision from the Brussels Court of First Instance on 16 February 2018.

#### **18.2 What “hot topics” are currently a focus for the data protection regulator?**

The Commission for the Protection of Privacy has recently been focusing on the following “hot-topics”:

- GDPR readiness: the Commission for the Protection of Privacy has been preparing for 25 May 2018 and the creation of the new Data Protection Authority;
- GDPR compliance: the Commission for the Protection of Privacy has put a lot of effort into raising awareness with and educating (i) businesses, large and small, on their obligations under the GDPR, and (ii) citizens on their (new) rights under the GDPR in connection with the processing of personal data;
- the privacy of minors: the Commission for the Protection of Privacy has been raising awareness among young people concerning the protection of their privacy online;
- image rights: the Commission for the Protection of Privacy developed the theme of image rights, both towards young people and their parents; and
- the fight against terrorism and violent radicalism: the Commission for the Protection of Privacy issued several opinions on the issue.



**Bastiaan Bruyndonckx**

Lydian  
Avenue du Port 86C b113  
1000 Brussels  
Belgium

Tel: +32 2 787 90 93  
Email: [bastiaan.bruyndonckx@lydian.be](mailto:bastiaan.bruyndonckx@lydian.be)  
URL: [www.lydian.be](http://www.lydian.be)

Bastiaan 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 companies in 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* and *Bulletin des Assurances*. Bastiaan recently 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.

**Olivia Santantonio**

Lydian  
Avenue du Port 86C b113  
1000 Brussels  
Belgium

Tel: +32 2 787 90 07  
Email: [olivia.santantonio@lydian.be](mailto:olivia.santantonio@lydian.be)  
URL: [www.lydian.be](http://www.lydian.be)

Olivia is a Senior Associate 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 often drafts and reviews privacy policies as well as data processing agreements. She also specialises in global privacy issues (GDPR compliance, contracts review, corporate binding rules, etc.).

Olivia is regularly invited as a speaker at conferences and seminars, including on the GDPR.

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

Our Information Governance & Data Protection (Privacy) team represents clients, large and small, from all industry sectors (including technology, retail, telecommunications, health care 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 client 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 data protection, such as Berwin Leighton Paisner, Burges Salmon, Hogan Lovells, Luther, Norton Rose Fulbright, Taylor Wessing and Willkie Farr & Gallagher.

# Brazil

Vaz E Dias Advogados & Associados

José Carlos Vaz E Dias



## 1 Relevant Legislation and Competent Authorities

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

There is no sole specific piece of legislation that deals with data protection. Any collection, storage, retention, treatment and use of personal data is ruled by different pieces of legislation scattered over diverse areas of law, applicable to different and specific groups of people and activities.

Nevertheless, there are three (3) pieces of prominent legislation that set the foundation for the recognition of personal rights and the protection of data. The first one is the Federal Constitution, which recognises privacy, private life, honour and the image of a person as essential to human existence and nature. In this sense, Item X of Article 5 of the Federal Constitution determines that private life and intimacy and image rights are inviolable and they can never be waived by their owner.

As a result, any intimate or expression of private life and personality is legally secured to individuals, including those related to professional and commercial relationships not exposed to the public by any means.

Moreover, a related matter is the confidentiality of data in correspondences and transmissions (including telephone communications and others) expressed in Item XII of Article 5 of the Federal Constitution.

Accordingly, the information contents of correspondences and data as well as the transmission of data are classified as confidential and inviolable, except in the event of a court order for the disclosure of such or others prescribed by law. This principle is regarded as complementary to the private life principle and encompasses situations related to business and commerce, such as data exclusivity and confidentiality rights.

On the other hand, the Federal Constitution secures to any citizen through Item XIV of Article 5 the right to access information – the so-called Right of Information – facts, people and situations in daily life, including checking the truth of facts. Such right also includes the possibility to make public information about facts and people, except those protected by confidentiality.

Both the inviolability of private life and the right of information are frequently examined in court in order to assert individual rights and prevent censorship and violation of confidentiality. Since they are, in principle, opposing principles, many discussions have been held on which principle should prevail to address data protection, especially regarding the internet, and how to establish checks and balances for the enforcement of the principles without jeopardising privacy.

The second relevant piece of legislation is Law 10,406 of January 10, 2002 (the so-called “Brazilian Civil Code” or “Law of the Common Man”) that revised concepts established by the Civil Code of 1916, adopted new principles and took into consideration new human and business relationships. This law established for the first time a specific section – Chapter II of Title I of Book I – comprising 11 articles ruling about privacy, private life, honour and the image of a person (so-called personality rights). There is a clear objective to protect the moral integrity of a person against possible third-party interference or unauthorised use of third parties. Therefore, legal measure may be granted to prevent violation of private life. The Brazilian Civil Code further recognises that personal situations can be only exposed by the decision of individuals owning the rights and in some specific situations, such as court orders for such.

Both pieces of legislation apply to Brazilian citizens as well as Brazilians and foreigners living in Brazil and companies and private organisations doing business or exercising their rights in the territory.

The third general piece of legislation is the Criminal Code (Decree-Law 2,848 of December 7, 1940), which provides in its Articles 150–154 for offences for disclosing information regarding residence, private location, private correspondences and messages, and information regarded as of a confidential nature. A new offence was added to the Criminal Code in 2012 (by Law 12,737 of November 30, 2012) related to the private life of individuals. Accordingly, it is an offence for a person to invade or hack computers or devices with the purpose to obtain, collect, display or destroy data or information without the authorisation of the holder. The penalty is up to two (2) years of imprisonment.

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

There is no single statute establishing the general civil rights framework for data protection in Brazil. However, Federal Law 12,965 of April 23, 2014 (known as the “Internet Law”) and its regulation (Decree 8,771 of May 11, 2016) are relevant to data protection.

The Internet Law establishes the principles, rights and obligations regarding the use of the internet in Brazil. It deals with the relationship between the provider and the internet user. Further, this law addresses the collection, storage, use and grant to third parties of access to private data through the internet (connection logs to which this law relates). It ensures that the contents of private communications and transfers comply with the protection of privacy, private life, honour and the image of the involved parties.

The Internet Law is recognised as of utmost importance to data protection in view of the increasing use of information stored and

transmitted electronically and business transactions made online. According to research published in 2017, Brazil had nearly 140 million internet users in 2016. Additionally, monthly internet usage in Brazil amounted to 25.7 hours per user in 2017 and 90% of Brazilian internet users accessed the internet every day for personal reasons (<https://www.statista.com/topics/2045/internet-usage-in-brazil/>). Therefore, the internet and worldwide web is a powerful tool used in Brazil for producing and transferring personal data, especially in commerce.

Federal Law 12,527 of November 18, 2011 (Freedom of Information Act) is also relevant. This law establishes procedures to be complied with by public agencies, the Federal Government, the Federal States, the Federal District and municipalities in order to ensure the access to information of private interest is available through public agencies. It rules the rights set out in Item XIV and also Item XXXIII of Article 5 of the Federal Constitution (so-called Habeas Data).

Additionally, the Bill of Law 5,276 of 2016 (Personal Data Protection Bill) is in the parliamentary process, and deals directly and consistently with the treatment and protection of personal data. The Personal Data Protection Bill expresses the most recent view of the community on the protection of personal data, as it shapes data protection dealing with private information and secures the free development of the personality and dignity of natural persons.

The Consumer Rights Code, Federal Law 8,078 of September 11, 1990, addresses the collection and use of consumers' data used for business and commerce. Paragraph 2 of Article 43, for example, expressly determines that the creation of files and databases, and the registration of personal data and data related to commerce, should be prior communicated to consumers. Consumers will have full access to the registered and gathered information about him/her and can request the rectification of incorrect collected data. This rule derives directly from Item X of Article 5 of the Federal Constitution.

By means of Decree 7,962 of March 15, 2013, new specific rules were set out for those consumers that buy products or hire services through the internet. Such rules deal essentially with three (3) aspects of consumer rights: (i) clear information about the products and services provided by the supplier through the internet; (ii) transparent rules to consumers; and (iii) the right to regret and to cancel the transaction.

Further to that, Federal Law 13,543 of December 19, 2017 sets out the obligation for internet providers to disclose ostensive and clear information to consumers when offering services/products through the internet. In this regard, the law establishes that such disclosure should take place in characters that may be clearly viewed by consumers, with a font size not lower than 12.

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

There are a couple of pieces of legislation that affect data protection and that form the legal framework for data protection in Brazil. They are the following:

- (1) Item XXXIII of Article 5 and Item II of Paragraph 3 of Article 37 of the Federal Constitution (Habeas Data) – These grant to all persons the right to receive from public agencies information of private interest regarding such person or of collective or general interest stored in any public agency, except information whose secrecy is essential to the national security of society.
- (2) Federal Law 12,527 of November 18, 2011 (Freedom of Information Act) – This establishes procedures for all persons' and citizens' requests to public agencies for the contents of private information and data and updates and rectifies any incorrect information available in public databases.

- (3) Complementary Law 105 of January 10, 2001 (Financial Transaction Confidentiality) – This addresses confidentiality related to transactions and storage of private information performed by financial institutions operating in Brazil. The general rules include the obligation of financial institutions to maintain safe and secret any collected information of their active and passive transactions and services rendered. Further, it sets out that the disclosure of private information of a person may only when expressly provided by the person. It also establishes the exceptions to these rules when special events take place, such as illicit activities, smuggling, terrorism, money laundering and corruption, among others. It establishes fines and penalties for the breach of confidentiality.
- (4) Federal Law 9,279 of May 15, 1996 (Industrial Property Rights Law) – The Industrial Property Rights Law stipulates in its Article 195 specific events regarded as a violation of confidentiality information in trade. Item XIV of Article 195, for example, deals with the exploitation or use of clinical test data. Accordingly, the unauthorised exploitation and use of clinical tests or other undisclosed data whose preparation involves considerable effort and that were submitted to public agencies for obtaining approval for a product's commercialisation is a crime. This rule specifically addresses data exclusivity of clinical trials. Besides the fact that data exclusivity is an investment in the pharma industry, it is recognised that the collected data in clinical trials comprises personal information about people that participate in the trials, and is thereby regarded as personal data. Nevertheless, Item XIV of Article 195 lacks further legal developments.

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

Brazil does not have a general administration or commission that can ensure compliance with the data protection legislation. Nevertheless, the laws of the land empower specific public bodies that are responsible for monitoring, identifying possible violations and ensuring that data protection is fully observed. The Brazilian Central Bank and the Securities and Exchange Commission (CVM) are empowered by Article 9 of Complementary Law 105/2001 to monitor and provide full assistance to the Federal Prosecutor General to confirm and hamper the violation of the law and that of confidentiality of private data and transactions.

Under the Internet Law framework, Article 17 of Decree 8,771/2016 empowers three (3) agencies and commissions to monitor and secure transparency related to the internet services disposed by providers and the protection of data stored and transferred to third parties. The first is the Telecommunication Agency (ANATEL), which provides regulation, and monitors and examines infringements, including those related to privacy or personal documents of consumers stored and/or transmitted by telecommunication companies. The National Commission on Consumer Rights is entitled to monitor and verify possible violations of use of internet services by consumers, including the collection, storage and use of data protection. The same powers have been granted to the Administrative Council for the Defence of Competition (CADE) in matters related to antitrust activities linked to internet business.

Article 20 of the Internet Law establishes that the aforementioned agencies or commissions and other public entities will work in close cooperation to safeguard the rights of those who use the internet, especially related to the collection, storage and safe disposal of private data to third parties over the internet. They will follow the guidelines set by the Management Committee for the Internet in Brazil (CGIbr). Such cooperation is further demanded especially when violating activities are incurred by entities located overseas under the terms of Article 11 of the Internet Law.

## 2 Definitions

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

#### ■ “Personal Data”

This is defined by both the Freedom of Information Act and the Internet Law as a piece of compiled information or data related to an identified or identifiable natural person, including identifying numbers, location data or electronic identification when these are related to a person as well as that found in private communication exchanged over the internet.

#### ■ “Processing”

This expression means any operation carried out with personal data, including collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, archiving, storage, disposal, evaluation or control of information, communication, modification, transfer, dissemination or extraction of information of a personal nature.

#### ■ “Controller”

The term “Controller” is not found in the Brazilian legislation, especially under a broad understanding that involves a public authority to register, approve and control data protection. However, “Controller” may be understood under a limited concept as public agencies empowered to monitor, clear offences and ensure compliance with the specific applicable legislation to data protection, such as the Internet Law and the Financial Transaction Law.

#### ■ “Processor”

This term is not found in the applicable legislation but may be understood under the concept of the Data Protection Bill as a person (public and private entity) that can retrieve, upload and store personal data for monitoring and ensuring compliance with the applicable laws.

#### ■ “Data Subject”

This term is not found in the applicable legislation nor in the Personal Data Protection Bill. It may be understood under the concept of international data protection as the physical person which the private information relates to and identifies.

#### ■ “Sensitive Personal Data”

“Sensitive Personal Data” is not defined by the relevant law. It is regarded, however, by the Personal Data Protection Bill as any compiled information of a personal nature specifically related to race, ethnic origin, religious beliefs, political opinions, affiliation to trade unions or organisations of a religious kind, philosophical or political nature, health or sexual life or orientation data and genetic or biometric data.

#### ■ “Data Breach”

“Data Breach” encompasses under the concept of the applicable laws the following infringement events, especially set by the Internet Law.

- (1) The use, exploitation and disclosure of private/personal information without the express, free and informed consent of the person identified by it or in accordance with the cases provided by law, such as the court orders.
- (2) The transfer or access to third parties of private information for commercial purposes or not without the prior, express and clear consent of the person identified by it or in accordance with cases provided by law, such as the court orders.
- (3) The denial of access of private information to the identified person for revision, update, elimination and rectification purposes.

- (4) The supply of unclear and/or incomplete information about the policy on the collection, use, storage, processing and protection of users’ personal data and connected records and records of access to internet applications.

- (5) Retention and the making available to third parties of connections logs and access to internet applications logs as well personal data and the content of private communication without respect for privacy, private life, honour and the image of the parties that are directly or indirectly involved.

#### ■ Other key definitions – please specify (e.g., “Pseudonymous Data”, “Direct Personal Data”, “Indirect Personal Data”)

The laws of the land further provide the following expressions:

- (a) Anonymous data – data related to an unidentified physical person or which cannot be identified.
- (b) Classified information – information which is temporarily unavailable for public access due to its relevance to social and state security (concept provided by the Freedom of Information Act).
- (c) Primary information – quality of first-hand unfiltered information, retrieved from original sources.
- (d) Information provider – entity that provides access to the internet and that should be responsible for the retention of records (connection logs, personal data and the content of private communications).
- (e) Processing of personal data – any operation carried out with personal data, such as collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, archiving, storage, disposal, evaluation or control of information, communication, modification, transfer, dissemination or extraction.

## 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?

Data protection applies, as a general rule, to Brazilian citizens and foreigners living in Brazil and companies/public and private entities (national and foreign) doing business in Brazil.

Nevertheless, Paragraph 1 of Article 11 of the Internet Law sets out that any operation of collection, storage, retention and treatment of personal data or communication data by connection providers extends to entities located overseas, if at least one of such acts take place in the Brazilian territory.

Further to that, the Internet Law applies to foreign companies that collect data in Brazil and to the content of communications in relation to which at least one of the terminals is placed in Brazil or in case they offer services in Brazil or at least one member of the same economic group (internet service provider) is established in Brazil.

The Personal Data Protection Bill sets out in its Article 3 the territorial scope of data protection that will prevail when it becomes an applicable federal law. Accordingly, data protection will apply to any operation of collection, storage, upload, retrieval, use, disclosure and processing of private data undertaken by a natural person or a private or public legal person and entity, regardless of the country where its headquarters/residence is located and of the country where the database is maintained, as long as (i) the processing operation occurs in the national territory, or (ii) the processing of private data aims to offer or dispose goods or services in Brazil, or (iii) the involved private data is of individuals located in Brazil, and (iv) when the personal data is collected in the Brazilian territory.



## 4 Key Principles

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

#### ■ Transparency

The transparency of collected and stored information is a sacred principle deriving from Item X of Article 5 of the Federal Constitution. This Item protects private information and gives full access to the collected and stored data for possible update, modification and deletion by the involved person.

As a result, the Transparency Principle is mentioned in federal laws and regulations dealing with the data protection framework. For example, the Freedom of Information Act holds as a principle the “promotion of the development of a transparency culture within the Public Administration” and free access to the information held in databases of public agencies.

The Transparency Principle is further guaranteed in the Internet Law and its regulation. Items VI and VII of Article 7 of the Federal Law determine the need to supply clear and full information entailed in internet service agreements, setting forth the details on the protection of connection records and records of access to internet applications, as well as traffic management practices that may affect the quality of the service provided. Providers need to supply further clear and complete information on the collection, use, storage, processing and protection of personal data.

#### ■ Lawful basis for processing

The lawful basis for processing is a principle that shapes specific laws on data protection, especially Decree 8,771/2016 (regulating the Internet Law). It determines the need for internet providers (and those responsible for the transmission, switching or routing) to adopt transparent measures to clarify to the user the reasons for network management. It further recommends providers to adopt guidelines setting security standards for personal data and private communication, including processing, storage and disposal to the individual whose personal data is concerned.

The Freedom of Information Act also provides a lawful basis for establishing rules for processing and using private data by public bodies and government agencies.

#### ■ Purpose limitation

The Purpose Limitation Principle prevails in the existing data protection framework, as the upload, collection and use of information about a person, including that related to communication data, should be limited and directly related to the purpose for which it was retained, stored and used. In this matter, Article 12 of Decree 8,771/2016 clearly sets out that “*connection and applications providers must retain as little personal data, private communications and connection and access to application records as possible*”. In addition, it determines that the retained and stored information should be deleted after the purpose of its use is achieved and the set legal deadline for storing data protection (as stipulated in the Internet Law) is complied with.

Further, collection, use, storage, processing and protection of users’ personal data may take place when such acts are adequately justified, are not prohibited by the laws of the land and are specifically provided in the terms and conditions of the internet service agreement.

#### ■ Data minimisation

Both specific laws on data protection – the Internet Law and the Freedom of Information Act – set out rules dealing with the collection and storage of minimum personal data,

specifically related to the purpose of their use. The Freedom of Information Act sets out that the access, disclosure and processing of confidential information shall be limited to those who need to know it and who are properly certified, following the existing regulations without prejudice of the competencies of public agents authorised by law.

#### ■ Proportionality

The right to collect, store, retrieve and upload personal data and those linked to internet connection records and records of access to internet applications, among others, should be previously authorised by the individual. Such right needs to comprise actual, updated and limited information on the individual. As a matter of preservation of the proportionality principle, the Internet Law grants to individuals the right to update and eliminate personal data provided to a certain internet application.

The Consumer’s Right Law also establishes the need of consumers to receive accurate and true information about an individual when companies and entities collect or provide information about a consumer or operate a consumer database.

Consumers are also companies or legal entities when they receive products or services from a supplier. This definition is provided by the Consumer Rights Code, as follows: any individual or legal entity that obtains or uses products or services as an end-user. Therefore, private information at the consumer level also involves those of legal entities.

#### ■ Retention

The retention principle derives from the personal data protection principle applied by the Internet Law. It requires that the internet provider or holder of the internet connection or of personal data information must maintain the connection records (private information) under confidentiality and in a controlled and safe environment for a period of one (1) year in accordance with the regulation. The responsibility for the maintenance of the data information and connection during the aforementioned period cannot be transferred to third parties.

An administrative or police authority or the Public Prosecutor Attorney may require precautionary keeping of connection records for a longer period of one (1) year. Such precautionary keeping request needs to be followed by a 60-day period (as of the date of the first request) to commence court proceedings to request access to the records.

As for application access logs, the internet provider needs to maintain the application access logs under confidentiality and in a controlled and safe environment for six (6) months.

It is important to state that the retention and the making available of connections logs and access to internet applications logs to which this law refers, as well as personal data and the content of private communications, must comply with the protection of privacy, honour and the image of the parties that are directly or indirectly involved.

According to Article 15 of Decree 8,771/2016, private data should be kept in an interoperable and structured format, for easy access in case of court decision or in those events specified by law.

The Consumer Rights Code further stipulates in Paragraph 1 of Article 43 the prohibition to maintain negative data about consumers in a database for a period longer than five (5) years, independently of the fact that the consumer might still be in debt to the business.

#### ■ Other key principles – please specify

There are additional key principles provided by the Brazilian Internet Law and the Freedom of Information Act related to protection of personal data, as follows:

- 1) The principle of publicity as a general rule and secrecy as the exception – the principle guides public administration when holding personal data of individuals and has as its main purpose the guarantee of access to individuals and also companies/entities of any private information held by public entities and agencies.
- 2) Disclosure of information of a public interest principle – this principle is set out by the Freedom of Information Act and aims to secure access to information, especially that in the public interest, irrespective of requests from the owner or the identified individual.
- 3) Free speech principle – this is secured to individuals against possible fake and wrong information kept in a database or publicised to third parties.

## 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 right of any individual to access private information is extensively secured in Brazil by case law based on the right of privacy and private life provided by Item X of Clause 5 of the Brazilian Constitution.

Three (3) specific legislations on data protection specifically provide rules on this right, as follows:

- Freedom of Information Act – grants full access of individuals to their information held by public entities and agencies, as provided in Articles 5, 7 and 8 of the law. Further, any individual will have access to its private information, regardless of the secrecy classification, for the maximum period of one hundred (100) years, as counted from the date of its production, following the terms of Article 31, Paragraph 1, Item I.
- Consumer Rights Code – Article 43 grants to consumers access to companies' files and databases specifically created to compile information about them, their lives and habits.
- Internet Law – Article 11 and others secure to any individual full access to the information collected and stored by internet providers and others involving the individual.

Further, the Internet Law and the Consumer Rights Code establish the prior and express consent of the person as a requirement to access private data (individual and consumer data). Consent suffers restrictions when given by persons under 16 years of age, which is not recognised as valid and enforceable as a general rule. Consents provided by individuals from 16 to 18 years of age are valid when assisted by their parents or legal guardians empowered to give consent.

The service provider should understand consent as a specific agreement from the internet user as to the collection, storage, transfer and use of its data.

#### ■ Right to rectification of errors

The right to rectify errors and update information is guaranteed for an individual to access private information in files and specific databases and correct the data. The Consumer Rights Code provides in its Paragraph 3 of Article 43 a specific ruling on the rectification of errors. It allows consumers to correct immediately and eliminate imprecise and incorrect information in the database, including those provided by internet providers. When requested by a consumer, database holders will correct the information and communicate the requested alteration and elimination within five (5) working days as from the consumer's request.

The Freedom of Information Act also entitles any individual to rectify errors and eliminate them from files and database in public agencies and entities. This grant comes from Item III of Article 3 and Article 6 of this law, which state that protection of personal information shall observe its authenticity and integrity.

#### ■ Right to deletion/right to be forgotten

The Internet Law directly secures to internet users in Item X of Article 7 the ability for definitive elimination of any personal data disposed to a certain internet application at the end of the relationship between the internet user (individual) and the internet provider. Such right to delete does not prevail over mandatory log retention, as specified by the applicable laws and court orders.

The right to completely delete any information disposed over the internet at any time (right to be forgotten) is not addressed by the Internet Law and other applicable laws. Notwithstanding the aforementioned, the right to deletion information at any time and the right to be forgotten are common matters of court action. A relevant decision on the matter was processed at the Superior Court of Justice (STJ) on the Special Appeal n.1.316.921-RJ (2011/0307909-6). The decision issued on June 26, 2012 affirmed that Google Brasil Internet Ltda did not have the obligation to exclude from the search tools images and information that would be potentially illegal due to the freedom of operation principle secured by the Federal Constitution.

The right to deletion/right to be forgotten is yet an issue to be resolved, since this matter is under examination by the Federal Supreme Court (RE 1010606) and the decision is expected to be issued later this year.

Paragraph 3 of Article 43 of the Consumer Rights Code is interpreted extensively to accept consumers' requests to delete private information from databases or files held by companies, entities and associations of any nature that hold information on consumers.

#### ■ Right to object to processing

The processing of private information is not prohibited under Brazilian law, since the Federal Constitution preserves the freedom of information principle. However, the collection, use and disclosure of any information about individuals need to be previously and expressly informed to the involved person.

According to Item IX of Article 7 of the Internet Law, the express consent of the individual for the collection, use, storage and processing of personal data is required. This consent needs to be addressed and obtained through a specific separate contractual clause. Further, it is an obligation of internet providers to supply clear and complete information on the collection, use, storage, processing and protection of users' personal data.

The same rights are found in the Consumer Rights Code, including the express consent.

There are discussions about the validity period of the express consent and therefore whether the express consent may be terminated at any time by the individual, which will permit objections to the processing of information. The discussion lies on the fact that intimacy and the private life are regarded by Article 11 of the Civil Code as personality rights. Therefore, they cannot be transmitted or renounced and their exercise cannot be voluntarily limited. On the other hand, both the Internet Law and the Consumer Rights Code value the transparency principle, which provides that once the individual adheres to the "User Agreement and Privacy Policy", it needs to comply with its terms and conditions.

The common understanding is that individuals adhering to a specific "User Agreement and Privacy Policy" should comply with its terms and conditions, but provisions restricting

the prior consent for deletion, transfer of information to third parties and others rights secured by the law cannot be eliminated or disposed of by the involved parties (the individual and the provider). Therefore, such violations would grant the user the right to object to processing.

#### ■ **Right to restrict processing**

Both the Consumer Rights Code and the Internet Law secure to individuals the right to restrict processing, including non-disclosure to third parties of personal data, connection records and records of access to internet applications.

The exception to this right would take place in case individuals expressly and freely consent to the transfer of files to third parties or in accordance with the cases provided by law, such as court orders and access by the administrative authorities to recorded data regarding personal qualification, affiliation and address.

The Freedom of Information Act further establishes in Paragraph 3 of Article 31 that the individual's prior consent to transmit private information to third parties will not be required for the following situations:

- (i) matters involving medical prevention and diagnosis, when the individual is physically or legally incapable, and solely and exclusively to guarantee due medical treatment;
- (ii) production of statistics and scientific research of public or general interest as set by the legislation. Nevertheless, the disclosure of the individual to whom the information refers is prohibited;
- (iii) compliance with court orders;
- (iv) protection of human rights; or
- (v) protection of overwhelming public and general interest.

#### ■ **Right to data portability**

The laws of the land do not specifically address the right of internet providers and holders of files and databases to reuse collected personal data for services other than that the same holder or provider offers.

Nevertheless, the Internet Law sets the obligation of providers, retainers and holders of files on private data to stipulate to the individual clear and complete information on the collection, use, storage, processing and protection of the individual's personal data. Such collection and use should be duly justified and related to providers' activities and clearly addressed in the proposed "User Agreement and Privacy Policy".

Therefore, the right to data portability through the internet is possible insofar as the aforementioned requirements and conditions are adequately fulfilled.

The same rationale is applicable to collected and stored information on consumers, following the Consumer Rights Code.

#### ■ **Right to withdraw consent**

The laws of the land do not specifically address this matter. However, the withdrawal of consent is implied under Article 11 of the Civil Code, which sets out that personality rights cannot be renounced but may be licensed temporarily. Therefore, individuals may exercise the right to withdraw the consent given to a provider or holder of files or a database encompassing private data at any time in case of violation of private rights and intimacy.

When a contract to exploit a database is fully complied with by the licensee, the withdrawal consent will be accepted only in the cases provided in the contract, such as the "User Agreement and General Policy".

This is further and broadly addressed by Article 8 of the Internet Law, since the guarantee to the right of privacy, private data and freedom of speech in the communications is a condition for

the full exercise of the right to access the internet. Therefore, contractual clauses in "User Authorisation and Privacy Policies" that violate the inviolability and secrecy of information are viewed as abusive and a breach of the right of privacy.

#### ■ **Right to object to marketing**

Individuals have the right to object to marketing to prevent their personal data being exploited in the market without the individual's express and prior consent. As a result, the individual may grant access to its private information to providers, holders of files and databases and establish restrictive use of this private data, excluding use for specific purposes or maintain the right to prevent marketing and other activities.

#### ■ **Right to complain to the relevant data protection authority(ies)**

Local laws do not specifically address the right to complain to the relevant data protection authority. Therefore, notification of public or regulating agencies is not needed for reporting data security breaches.

The Federal Constitution grants to any individual access to court actions and to petition the government authorities in defence of rights or against illegal acts or abuse of power.

The Freedom of Information Act further secures this right. As for the Internet Law, Article 17 of Decree 8,771/2016 lists specific public agencies involved in the provision of internet access that act in the regulation, monitoring and verification of infringements, as follows:

- the National Secretariat of Consumers, which monitors and verifies the infringement of consumer rights;
- the Brazilian Council for the Defence of Competition (CADE), which monitors the effects of the Internet Law on competition; and
- other organisations and entities of the federal public administration with specific competence, including the Steering Committee of Internet (CGI.br).

## 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 applicable laws on data protection do not prescribe registration of private information or data protection before any agencies or authorities.

### 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 information does not apply to Brazil. No registration or notification is needed for data protection. The Personal Data Protection Bill does not stipulate registration at public agencies.

### 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 Brazil. See the answers to questions 6.1 and 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)?**

Neither the current laws nor the Bill addresses the registration of data protection and the creation of registration authorities.

**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 Brazil.

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

This is not applicable in Brazil, as individual information is of a private nature and extensively protected under the Federal Constitution and specific laws, without any registration or recognition requirements.

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

This is not applicable in Brazil.

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

This is not applicable in Brazil.

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

This is not applicable in Brazil.

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

This is not applicable in Brazil.

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

This is not applicable in Brazil.

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

This is not applicable in Brazil.

## 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 concept of a Data Protection Officer is not dealt with by existing

data protection law in Brazil. Therefore, this authority does not exist under the laws of the land.

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

This is not applicable in Brazil.

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

This is not applicable in Brazil.

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

This is not applicable in Brazil.

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

This is not applicable in Brazil.

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

This is not applicable in Brazil.

**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 Brazil.

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

This is not applicable in Brazil.

## 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 existing applicable data protection laws do not address the issues related to the processing of personal data by a processor as opposed to companies or entities for the collection, upload, retrieval and storage of personal data. Therefore, agreements between businesses and processors are matters of a commercial nature.

Nevertheless, internet users need to obtain clear and full information entailed from the "User Agreement" and any other agreement related to internet services (executed between the business and the internet user) about the details of how collection, use, storage, processing and protection of its personal data will take place. Further, adequate information on the protection of connection records and records of access to internet applications should be provided.



This means that internet users need to obtain clear information about the processor (name, address, taxpayer number, etc.) that will process its personal data, the conditions of access to the private information and assurances that the personal data will be fully respected by the processor. In this regard, internet users may oppose the execution of an agreement between a business and processor in the sense that it may refuse to give access to its private data in case it is not adequately and clearly informed about the processor and in case of an agreement between businesses.

Further, agreements between businesses and processors may be void in case they contain clauses that are an offence against the inviolability and secrecy of private communications or, in case of adhesion contracts, they do not provide an alternative to the contracting party to adopt the Brazilian courts for resolution of disputes arising from services rendered in Brazil. See Clause 8, Sole Paragraph, Items I and II of the Internet Law. In addition, clauses that restrict any user's right to access to its own private data are not enforceable.

The same requirement applies to private information on consumers, contractual clients and fiscal information, since all of these are ruled by the inviolability of intimacy and private life.

---

**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 Brazilian Internet Law and other applicable laws (including the Civil Code) do not address the formalities of commercial agreements between businesses and processors. This raises the possibility to adopt an electronic agreement instead of a formal written agreement. Accordingly, electronic agreements may be adopted insofar as the internet user obtains the following assurances regarding protection of personal data collected and used through the internet:

- Assurance of the inviolability of the intimacy and private life of the internet user.
- Assurance of the inviolability and secrecy of the flow of the user's communications through the internet.
- Supply of clear and full information entailed in the services agreements that set forth details concerning the protection of connection records and records of access to internet applications.
- Provision of adequate information about the mechanisms that will be used to secure the confidentiality and inviolability of the user's private information.
- Provision of guidelines on the processing and safeguarding of the collected private information.
- Specification of the provider's obligations regarding the maintenance of connection records, including the assurance of the business' and provider's responsibility for the maintenance of such connection records, since such responsibility cannot be transferred to third parties.

As for the formalities of such agreements, the consent of the internet user for access to the service provider is required to be clear. The mere use of the device that transmits information electronically or the use of the internet services is not evidence of the user's express consent to the collection, storage, transfer and use of its data by the service provider. It is required that the consent is specifically requested and given by the internet user.

Moreover, the internet user needs to obtain adequate information about the processing of data by a processor and the maintenance of connection records and must duly approve such access to its personal data and connection by the processor (as a third party).

Due to its access to the user's private information, a processor hired by a business will be liable for any damages caused by the processing of the internet user's private data. Businesses will be jointly liable with processors only if provided in their 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?)**

---

There is no specific legislation ruling and/or establishing restrictions on sending electronic direct marketing by email or SMS. Therefore, privacy principles, regulations and case law on advertising applies to direct marketing.

Regarding the privacy principle, we note the need for internet providers to respect the intimacy and private life of users, maintain the secrecy of their communications over the internet and adequately and safely store their private communications. The Internet Law allows the collection and storage of private data to be in the scope of an internet provider's specific commercial purposes.

Regarding advertising regulations, direct contact for marketing purposes to a consumer at home or work may be classified as illegal and abusive, under Item IV of Article 6 of the Consumer Rights Code, when undertaken through dishonest and coercive business methods and without the consumer's prior approval.

Further, electronic direct marketing to subscribers or individuals and companies who previously objected to such marketing is prohibited.

---

**9.2 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 no specific legislation addressing restrictions on marketing via other business means. Therefore, the general prevailing principles on intimacy and regulations and case law on advertising apply.

Marketing via telephone, post, SMS and other means is prohibited when these are undertaken through dishonest and coercive business methods or to subscribers who previously objected to such marketing.

---

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

---

The general prevailing principles on intimacy and regulations on advertising also apply to marketing sent from other jurisdictions to Brazilian clients. The Consumer Rights Code is a public order law and court actions based on the violation of marketing rights need to be fully respected, notwithstanding the fact that the defendant is a foreign company.

Further, the international treaties executed by Brazil will be fully observed. Article 3 of the Internet Law expressly states that the law does not exclude matters agreed in international treaties.

Further, foreign acts, procedures and decisions, and any declarations, are not enforceable in Brazil when they violate public order laws, national sovereignty and good conduct in accordance with Article 17 of Decree-Law 4,657 of September 4, 1942 (Law of Introduction to the Rules of Brazilian Law).

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

There is no public authority in charge of enforcement of breaches of marketing restrictions.

#### 9.5 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 from third parties is not prohibited under the applicable laws insofar as the individual, company or entity under which the private data is traded expressly authorise the transfer of the files and information to a third party. Further, a third party needs to implement adequate security measures, as provided by Articles 7, 8, 11, 12, 13, 14, 15, 16 and 17 of the Internet Law.

The Consumer Rights Code further establishes abusive and unfair commercial practices, including those not in accordance with the Code, as an offence.

#### 9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

Sending marketing communications in breach of the Brazilian Internet Law may be subject to losses and damages and the following penalties:

- Warning.
- Fines of up to 10% of the revenue of the company or internet provider in Brazil.
- Suspension or prohibition of data collection and storage activities.

## 10 Cookies

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

Data protection legislation does not address the use of cookies or other similar technologies. Therefore, cookies are permitted insofar as this mechanism of collecting private information complies with the following requirements:

- prior and/or express consent of the person is adequately given; and
- storage and keeping of connection records, and the security and confidentiality measures are informed to the individual, as provided by the Brazilian Internet Law and Consumer Rights Code.

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

There is no law with provisions regarding cookies and therefore the general rules on intimacy rights and consumer rights apply. Where cookies do not identify the individual but gather general information about individuals and consumers without distinguishing them, prior consent and the rules provided in Clauses 7, 8, 10, 11, 14, 15, 16 and 17 of the Brazilian Internet Law do not apply.

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

This question does not apply, since there is no data protection authority applicable to regulate cookies.

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

The answers provided in question 9.6 above apply to the breach of applicable cookie restrictions.

## 11 Restrictions on International Data Transfers

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

There are no existing restrictions on the transfer of personal data to other jurisdictions. Therefore, such restrictions are the same as those applicable to the transfer of information to any third party, as provided in our answers to questions 8.1 and 8.2 above.

#### 11.2 Please describe the mechanisms companies 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 our knowledge, the following procedures must be complied with in the transfer of local personal data to other countries:

- Execution of an assignment agreement.
- Compliance with the foreign exchange control laws and taxation applicable in case payment for the transfer of private data to foreign parties takes place.
- Provision of guidelines or detailed information to the individual about the storage and use of their data, including access logs to connections and internet applications records.
- Provision of the assignment agreements rules set by the Internet Law, as these are indispensable for the transfer of files and access to information by third parties.
- Provision of adequate and clear information to the individual about the foreign rules that will be applicable to the transfer of their personal data that may affect the validity and enforceability of their data protection rights.

As a result, the transfer of personal data to other countries will require compliance with the transparency and prior and written consent rules and the provision of adequate information to the individual to which the personal data refers.

#### 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 or notification related to the approval of the transfer of personal data to other jurisdictions.

## 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.)?

Federal Law 13,608 of January 11, 2018 authorised the set-up of hotlines to receive reports and rewards for information that support police investigations in the prevention and repression of crimes or administrative offences.

This Federal Law further sets out the obligations of transport companies that operate under concessions by the federal, state and municipal government to exhibit in their vehicles a “Dial Complaint” sign, thereby permitting complaints of any kind that may assist police investigations about existing facts.

One of the most important rulings of this law is the guarantee that informants will have their name and private data kept fully confidential, therefore complying with the inviolability of privacy and private life assured by the Federal Constitution.

Although Brazil does not have specific ruling and laws, besides Federal Law 13,608/2018, dealing with whistle-blower hotlines, it is recognised that companies and public and private entities may adopt such programmes. However, private data of informants and those reported in the investigation should be kept confidential until the criminal offence is confirmed and made public by the authorities.

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

Anonymous reporting is generally permitted; taking into account that the information or the provided report aims to assist the investigation about the veracity of the facts, corporate anonymous reports should be published with great care so that private information, especially those not related to the report and names of people, are not unduly made public.

## 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 regulation in Brazil dealing with CCTV systems that record people in public or private areas. Therefore, there is no data protection authority or rules dealing with specific forms of public notice.

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

CCTV recording requires compliance with the inviolability of intimacy and private life principles and the need to use such CCTV strictly for its intended purpose in a specific place. If CCTV data is collected for checking possible trespassing, it cannot be used for other purposes.

## 14 Employee Monitoring

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

Employee monitoring or surveillance is not regulated under Brazilian law. It is shaped instead by case law and scholars’ reasoning, which allow such practices insofar as the employee’s privacy rights (also encompassed by Item X of Article 5 of the Federal Constitution) are not violated and the adopted surveillance measures are justified and applied proportionally for achieving the proposed objectives. Therefore, monitoring employees to protect the company’s property and competitive information regarding trade secrets is fully acceptable. But it is recommended that monitoring procedures and measures be adequately and clearly informed to the employees, including access to the companies’ computers and emails.

Labour courts understand that personal devices (bags, purses, etc.) are covered by an employee’s right to privacy. Therefore, a company must obtain free and informed consent from the employee to monitor and access personal devices, and/or letting them know that monitoring and searches may occur in specific situations.

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

Access to devices owned by the company in use by its employees does not require prior consent, but employees should be always informed that the work devices are of a professional nature not private. Therefore, it is recommended for a company to tailor specific guidelines to ensure that employees clearly know the boundaries between private information and the company’s information and access to such.

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

No work council, trade representatives or trade unions need to be notified or consulted to adopt surveillance measures, as the monitoring of employees is not regulated by law.

## 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 Internet Law, by means of Decree 8,771/2016, sets standards for security and confidentiality of records, personal data and private communications over the internet. The standards aim to prevent undue transfer of private information and the flow of a user’s communication over the internet to third parties and secure information for possible courts’ and public authorities’ use related to monitoring and infringement of rights.

Accordingly, the provider responsible for the retention of private records and/or data will only be obliged to provide them, separately or in association with personal data or other information that permits the identification of the user or of the internet terminal, by court order and other provisions dealt with by the law.

Further, the provider should observe standard security guidelines concerning the possession, storage and processing of personal data and private communications. Among them, we highlight the need to:

- (i) Establish strict control over access to data by creating responsibilities for those who have access and exclusive access privileges for certain users.
- (ii) Create detailed access logs for connection and internet applications records.
- (iii) Use management solutions for records of collected information that secures the inviolability of the collected data, such as encryption or related measures.
- (iv) Delete private information after the purpose of collection, storage, retrieval and use has been achieved or after the deadline determined by the legal obligation has come due.

As for keeping connection records, Article 13 of the Internet Law sets out that the provider or entity responsible for the management of an autonomous data system must keep the connection records confidential and in a controlled and safe environment for a maximum period of one (1) year. Administrative and police authorities or the Public Prosecutor may require precautionary keeping of connection records for a longer period.

The responsibility for the maintenance of such connection records cannot be transferred to third parties.

The Internet Steering Committee is responsible for the promotion of studies and recommendation of procedures, as well as for setting technical and operational standards for the better security and confidentiality of records, personal data and private communications.

In view of the importance of confidentiality, Paragraph 2 of Article 13 of Decree 8,771/2016 establishes that internet providers must retain as little personal data, private communications, and connection and internet applications records as possible.

There are no related provisions and requirements in other relevant laws for data protection.

**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) expects voluntary breach reporting.**

In accordance with the applicable laws, private data breaches do not have to be reported to any public or private authorities. Once any infringement of private data or non-compliance by internet providers and similar in keeping records of access to internet applications is noticed, the infringed individuals may proceed in court and recover any losses and damages suffered from the internet provider or third parties involved in the infringement.

Any reports related to breaches of private data may be obtained directly through the agencies responsible for the supervision and verification of data infringement. Such report has the objective to assist the agencies in drafting policies and making improvements to the system.

**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) expects voluntary breach reporting.**

There are no legal requirements to report data breaches to affected data

subjects in accordance with existing legislation on data protection. The infringement of private data is dealt with by the courts and no penalties are set by administrative public or private authorities.

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

The violation of data security grants to the affected individual compensation for losses and damages suffered. The amounts given for losses and damages will be stipulated by the judge in proportion to the extent of the damages.

The Internet Law has not set any criminal penalties for data security breaches.

Further, the following sanctions will be applied to internet providers or retainers of private information following the provisions of the Internet Law:

- (i) A warning, which shall establish a deadline for the adoption of corrective measures.
- (ii) A fine of up to 10% of the gross income of the economic group in Brazil in the last fiscal year.
- (iii) Temporary suspension of activities.

In case a foreign company violates such rights, the Brazilian subsidiary, branch or office will be held jointly responsible for the payment of the applicable fines.

There are no specific rulings related to the collection, storage and use of sensitive data of employees and customers (consumers) which may raise rights to compensation based on material and moral damages.

## 16 Enforcement and Sanctions

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

This is not applicable in Brazil.

**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?**

Brazilian legislation has no data protection authority for the establishment, function and enforcement of the applicable laws. Existing public agencies listed in Decree 8,771/2016 (regulating the Internet Law) are empowered to monitor and regulate the observance of the applicable laws regarding data protection, such as consumer rights, antitrust and telecommunications.

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

This is not applicable in Brazil, as no authority has been empowered to monitor and enforce data protection.

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

This is not applicable in Brazil. Please see our answer to question 16.2 above.



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

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

Brazilian companies are required to respond to e-discovery requests by providing adequate information on electronic data that may be used as evidence of criminal or civil charges. Adequate information means answering the questions in the e-discovery requests and providing full access to any private data specified in the e-discovery. Nevertheless, the delivery of information and data needs to be supported by a court order. In this matter, we highlight that the use, disclosure and transfer of private data to any third parties needs to be expressly authorised by the individual to which the private information relates or, as an exception, by a court order in case of possible infringement of data protection.

Further, e-discovery requests have to comply with the procedures of the Brazilian Civil Procedural Code, which requires confirmation of the country in which the plaintiff of the source of the e-discovery request is located. Also, the fulfilment of formalities should be confirmed, such as giving notice or summoning through Letters Rogatory.

Foreign companies may also service notices (so-called *notificação extrajudicial*) to Brazilian companies for e-discovery, but such notices are considered to be for private purposes. They are not recognised as effective instruments for giving notice or summoning Brazilian companies for court proceedings.

Brazilian companies follow the same procedures and request for disclosure through foreign courts and procedures.

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

Brazilian law does not provide a data protection authority. Please see our answer to question 16.2 above.

## 18 Trends and Developments

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

A recent enforcement trend relates to the acceptance of examination and judgment in the Federal Supreme Court of Brazil (STF) of a case related to the right to be forgotten (case no. RE 1010606). This court action does not involve internet service providers, but TV channels. It further deals with the opposition of two constitutional principles: the freedom of speech and the right to private life. The decision, to be issued most probably this year, will certainly extensively influence sectors that have as their main purpose the collection, storage, retrieval, use and exercise of private data, such as those involving internet services, consumer rights and entertainment rights.

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

The biggest issue for data protection regulators and/or judges for 2018 is the legal treatment of “fake news”, in view of the general elections for the presidency and the Federal Members of Parliament, which will take place in October/November 2018.

Very recently, the Federal Government and the local press have been complaining about the amount of fake news on the death of a member of Rio de Janeiro’s parliament – Mrs. Marielle – who was assassinated by “hired people” on March 14, 2018. Most of the fake news has been attempting to relate her death to drug trafficking or paramilitary groups. It is believed, however, that her assassination occurred due to her activities in favour of the poor and black people and against police abuse.

Although the Internet Law has provided adequate protection to several issues related to data protection, fake news and its sometimes devastating effects are issues which concern the authorities and legislators. Judicial authorities have called on Congress to pass comprehensive rules dealing with fake news and penalties for publishing such that affect the electoral process, public safety and public health.

**José Carlos Vaz E Dias**

Vaz E Dias Advogados & Associados  
Rua da Assembleia 10  
Conjuntos 1503/1504  
Centro, Rio De Janeiro  
Brazil

*Tel:* +55 21 3176 6530

*Email:* jose.dias@vdav.com.br

*URL:* www.vdav.com.br

José Carlos Vaz e Dias is an attorney-at-law, and has been specialised in intellectual property law since 1990 and is a partner of the intellectual property law firm **VAZ E DIAS ADVOGADOS & ASSOCIADOS**. His expertise includes the enforcement of patents, know-how and repression of unfair competition activities. He has special knowledge on licensing agreements of intellectual property, personality rights, data protection, sports law and entertainment law, regarding which he provides legal support to artists and sportsmen.

José Carlos Vaz e Dias holds an LL.M. and a Ph.D. from the University of Kent in Canterbury (England). He is also a Professor of the State University of Rio de Janeiro (UERJ) where he teaches intellectual property rights law.



**VAZ E DIAS ADVOGADOS & ASSOCIADOS**

The law firm **VAZ E DIAS ADVOGADOS & ASSOCIADOS** is specialised in intellectual property law and focuses on assisting foreign and local companies in the protection of intangibles and providing legal support for business transactions that explore intellectual knowledge and technological innovation. The firm's legal activities also involve the legal support on the protection and exploitation of image and personality rights, especially of actors, sportsmen and those who allow the exploitation of their image rights by the media. The firm is further involved in the implementation of confidentiality and data protection policies for the guarantee of secret information and the access of private information, commercial pledge of intellectual property rights, assignment of trademarks and patents, technology transfer and licensing agreements, franchising, image rights usage, copyright and entertainment law. The firm's legal activities encompass aspects related to the protection of technological inventions through patents and utility models, to the registration of industrial design, plant varieties, semiconductors, trademarks, domain names, copyright and their efficacy in the Brazilian territory, and entertainment and personality law.

# Canada

Osler, Hoskin & Harcourt LLP

Adam Kardash



Patricia Kosseim



## 1 Relevant Legislation and Competent Authorities

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

#### Private Sector Privacy Laws in Canada

There are four private sector privacy statutes that govern the collection, use, disclosure and management of personal information in Canada: (i) the Federal *Personal Information Protection and Electronic Documents Act*, S.C. 2000, ch. 5 (“PIPEDA”); (ii) Alberta’s *Personal Information Protection Act*, S.A. 2003, ch. P-6.5 (“PIPA Alberta”); (iii) British Columbia’s *Personal Information Protection Act*, S.B.C. 2003, ch. 63 (“PIPA BC”); and (iv) Québec’s *An Act Respecting the Protection of Personal Information in the Private Sector*, R.S.Q., ch. P-39.1 (“Québec Privacy Act”). Collectively, these will be referred to hereinafter as the “Canadian Privacy Statutes” and will be the main focus of this chapter.

The Federal private sector law, PIPEDA, governs the inter-provincial and international collection, use and disclosure of personal information. It applies to personal information (including employee information) held by federally regulated businesses, such as banks, airlines, railways, telecommunications companies and internet service providers, across the country.

PIPEDA also applies generally to personal information (excluding employee information) that is collected, used and disclosed by organisations in the course of a commercial activity which takes place *within* a province that does not otherwise have “substantially similar” legislation.

The private sector privacy statutes in Alberta, British Columbia and Québec (referenced above) have each been deemed “substantially similar” to PIPEDA and, as such, PIPEDA will not apply to commercial organisations operating *within* those jurisdictions, other than federally-regulated businesses which continue to be covered by PIPEDA regardless.

The health privacy statutes in Ontario, New Brunswick, Newfoundland & Labrador and Nova Scotia have also been deemed substantially similar to PIPEDA, and therefore, PIPEDA does not apply in respect of private health providers operating *within* those jurisdictions but continues to apply to other commercial activity therein. (See the response to question 1.3 for information on health privacy legislation in Canada.)

#### Public Sector Privacy Laws in Canada

Federal, provincial and territorial laws otherwise govern all public sector institutions within each of their respective jurisdictions.

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

Canada has enacted anti-spam legislation entitled *An 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*, S.C. 2010, c. 23 (“Canada’s anti-spam legislation” or “CASL”). (See the response to question 9.1 for details.)

British Columbia (*Privacy Act*, R.S.B.C. 1996, c. 373), Saskatchewan (*The Privacy Act*, R.S.S. 1978 c. Chapter P-24), Manitoba (*Privacy Act*, C.C.S.M., c. P125) and Newfoundland and Labrador (*Privacy Act*, RSNL1990, c. P-22) have also each adopted a statutory tort of invasion of privacy.

Québec civil law also provides individuals with a right to privacy under the *Civil Code of Québec*, CQLR, c. CCQ-1991 and the *Québec Charter of Human Rights and Freedoms*, CQLR, c. C-12.

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

Yes. Most of the provinces in Canada have enacted health privacy legislation that applies to health information custodians in the context of providing healthcare services.

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

Each Canadian jurisdiction – federally, provincially and territorially – has its own independent Information and Privacy Commissioner who reports to their respective legislature and oversees the relevant data protection laws applicable in that jurisdiction.

## 2 Definitions

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

#### ■ “Personal Data”

“Personal Data” (“Personal Information”) is defined very broadly under Canadian Privacy Statutes as information

about an identifiable individual. Generally, information will be deemed to be about an “identifiable individual” where it is reasonably possible for an individual to be identified through the use of that information, alone or in combination with other available information.

- **“Processing”**  
“Processing” is not expressly defined under Canadian Privacy Statutes but, in practice, would include the collection, use, modification, storage, disclosure or destruction of personal information.
- **“Controller”**  
“Controller” is not expressly defined under Canadian Privacy Statutes. Canadian Privacy Statutes refer to “organizations” more generally, which include controllers.
- **“Processor”**  
“Processor” is not defined under Canadian Privacy Statutes. Canadian Privacy Statutes refer to “organizations” more generally, which include processors.
- **“Data Subject”**  
“Data Subject” is not defined under Canadian Privacy Statutes. Canadian Privacy Statutes refer to individuals.
- **“Sensitive Personal Data”**  
“Sensitive Personal Data” is not defined under Canadian Privacy Statutes. PIPEDA provides that “any information can be sensitive depending on the context”.
- **“Data Breach”**  
PIPEDA defines a “breach of security safeguards” as “the loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of an organization’s safeguards that are referred to in clause 4.7 of Schedule 1 or from a failure to establish those safeguards”.  
PIPA AB does not define “Data Breach” but requires notification to the Alberta Information and Privacy Commissioner who may in turn require notification to affected individuals “of any incident involving the loss of, or unauthorized access to, or disclosure of, the personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure”.
- **Other key definitions – please specify (e.g., “Pseudonymous Data”, “Direct Personal Data”, “Indirect Personal Data”)**  
There are no other key definitions in particular.

### 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?

Although PIPEDA is silent with respect to its territorial reach, the Federal Court of Canada has found that PIPEDA will apply to businesses established in other jurisdictions if there is a “real and substantial connection” between the organisation’s activities and Canada. With respect to websites, relevant connecting factors include: (1) where promotional efforts are being targeted; (2) the location of end-users; (3) the source of the content on the website; (4) the location of the website operator; and (5) the location of the host server.

## 4 Key Principles

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

- **Transparency**  
Under the Transparency principle (also referred to as “Openness”), Canadian Privacy Statutes require organisations to document and make readily available to individuals, in a form that is generally understandable, specific information about their policies and practices relating to the management of personal information.
- **Lawful basis for processing**  
In general, Canadian Privacy Statutes require organisations to obtain consent for the collection, use and disclosure of personal information, subject to limited exceptions. In order for consent to be valid, it must be reasonable to expect that individuals would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting. An organisation shall not require consent, as a condition for providing a product or service, beyond that required to fulfil an explicitly specified and legitimate purpose. The form of consent (express or implied) may vary depending on the nature of the information and the reasonable expectations of the individual. Individuals may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice.  
Canadian Privacy Statutes contain a general obligation that personal information must be collected by fair and lawful means (i.e., consent must not be obtained through deception, coercion or misleading practices).  
Even with valid consent, organisations are subject to an overarching legal requirement that personal information can only be collected, used and disclosed for purposes that a reasonable person would consider appropriate in the circumstances. *See the Proportionality principle below.*
- **Purpose limitation**  
Organisations are generally required to identify the purposes for which personal information is collected at or before the time the information is collected. Organisations shall also document such purposes in accordance with the Transparency principle, *see above*.  
Personal information must not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. *See also the Data minimisation and Proportionality principles.*
- **Data minimisation**  
Canadian Privacy Statutes generally require that the collection, use and disclosure of personal information be limited (both in type and volume) to the extent to which it is necessary to fulfil the purposes identified by the organisation. Personal information shall not be retained longer than necessary to fulfil those purposes. *See the Retention principle, below.*
- **Proportionality**  
Canadian Privacy Statutes generally set out the overriding obligation that organisations may only collect, use and disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.  
The principle of proportionality is also built into some of the other principles. For example, the safeguarding obligation imposed on organisations is proportional to the level of sensitivity,



whereby the more sensitive the information, the higher the level of protection will be required. *See Safeguarding principle below.* Similarly, the extent to which personal information shall be accurate, complete and up to date will depend upon the use being made of the information, taking into account the interests of the individual. *See Accuracy principle below.*

#### ■ **Retention**

In keeping with the *Data Minimisation principle above*, Canadian Privacy Statutes generally require organisations to retain personal information for only as long as necessary to fulfil the purposes for which it was collected, subject to a valid legal requirement.

Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased or made anonymous.

Organisations should develop guidelines and implement procedures for retention of personal data, including minimum and maximum retention periods and procedures governing the destruction of data.

#### ■ *Other key principles – please specify*

**Accountability** – Canadian Privacy Statutes reflect the key principle of accountability. Organisations are responsible for protecting personal information under their control, including personal information that they transfer to third parties for processing, for which they must ensure a comparable level of protection through contractual or other means.

Organisations must designate and identify an individual who is accountable for the organisation's compliance with the other privacy principles and shall implement policies and practices to give effect to those principles.

**Safeguarding** – Each of the Canadian Privacy Statutes contains specific provisions relating to the safeguarding of personal information. In essence, these provisions require organisations to implement reasonable technical, physical and administrative measures to protect personal information against loss or theft, as well as unauthorised access, disclosure, copying, use, modification or destruction.

**Accuracy** – Canadian Privacy Statutes contain obligations for organisations to ensure that personal information in its records is accurate, complete and up to date, particularly where the information is used to make a decision about the individual to whom the information relates or is likely to be disclosed to another organisation.

## 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 Canadian Privacy Statutes, organisations must, upon request and subject to limited exemptions, inform individuals of the existence, use and disclosure of his or her personal information, and must give them access to that information, including a listing of the third-party organisations with whom the information has been shared.

The right of “access” does not oblige an organisation to provide copies of personal information records; rather, it requires the provision of access, which may include viewing the records at the organisation's offices. Generally, an individual's request must be sufficiently specific as to allow an organisation to identify responsive records. The organisation must respond within a prescribed time limit, or a reasonable period, as the case may be, at minimal or no cost to the individual, and must make the information available in a form that is generally understandable.

The exemptions to the right of access vary among the statutes and need to be carefully considered. Examples of the statutory exemptions include, but are not limited to, information subject to solicitor-client or litigation privilege, confidential commercial information, information about another individual, information that relates to national security matters and information generated in a formal dispute resolution process.

#### ■ **Right to rectification of errors**

Canadian Privacy Statutes generally require that when an individual demonstrates the inaccuracy or incompleteness of his or her personal information held by an organisation, the organisation must correct the inaccuracies and/or add a notation to the information, as appropriate.

#### ■ **Right to deletion/right to be forgotten**

While Canadian Privacy Statutes afford individuals the right to withdraw consent and challenge the accuracy, completeness and currency of their personal data, they do not grant a specific right to require organisations to “erase” or delete their personal information *per se*.

#### ■ **Right to object to processing**

Although Canadian Privacy Statutes do not include a specific right to object to processing, they do prohibit organisations from requiring, as a condition for providing a product or service, that individuals give consent to the collection, use or disclosure of their personal information beyond that which is required to fulfil the explicitly specified and legitimate purpose.

Also, an individual must be able to withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. Upon receipt of any withdrawal, individuals must be informed of the implications of such withdrawal.

#### ■ **Right to restrict processing**

*See above.*

#### ■ **Right to data portability**

Although Canadian Privacy Statutes include a right of access to personal information (*see above*), they do not include a right to data portability.

#### ■ **Right to withdraw consent**

Under Canadian Privacy Statutes, an individual must be able to withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. Individuals must be informed of the implications of such withdrawal.

#### ■ **Right to object to marketing**

Consent is required for the collection, use or disclosure of personal information for marketing purposes. The form of consent required (opt-in or opt-out) will vary depending on the circumstances, the sensitivity of the information and the reasonable expectations of the individual. In cases where opt-out consent is appropriate, individuals must be made aware of the marketing purposes at or before the time of collection, and in a manner that is clear and understandable. Individuals must be able to easily opt-out of the practice; the opt-out must take effect immediately and be persistent; and, the information collected and used must be destroyed or effectively de-identified as soon as possible thereafter. (*See also the response to question 9.1.*)

#### ■ **Right to complain to the relevant data protection authority(ies)**

Under Canadian Privacy Statutes, individuals have a right to make a complaint to the relevant data protection authority. Prior to this, individuals must be able to address data protection issues with the designated individual within the organisation who is accountable for the organisation's compliance. (*See Accountability principle above.*) Organisations must have easy-to-access and simple-to-use procedures in place to respond to complaints or inquiries and must take steps to effectively address complaints accordingly.

- *Other key rights – please specify*  
There are no other key rights in particular.

## 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, businesses do not have any legal obligation to register with or notify the relevant data protection regulatory authorities in respect of processing activities. Exceptionally, organisations that wish to use or disclose personal information without consent for statistical, or scholarly study or research, purposes must (in addition to other conditions) notify the Federal Privacy Commissioner before such use or disclosure.

*(See the response to question 15.2 for notification requirements in the event of data breaches.)*

- 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.**

PIPEDA, PIPA Alberta and PIPA BC expressly require organisations to appoint an individual who is accountable for ensuring compliance with the organisation's data protection obligations and who may, in turn, delegate some of his or her responsibilities to others. Such individuals are typically referred to as the Chief Privacy Officer or Privacy Officer, though Canadian Privacy Statutes do not prescribe any particular title.

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

There are no specific sanctions for failure to appoint a Privacy 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?**

Canadian Privacy Statutes do not protect Privacy Officers against disciplinary measures as a specific function of their role. However, Privacy Officers, like other employees, enjoy some protection against retaliatory action of their employer when they, acting in good faith and based on reasonable belief, refuse to do something that will contravene the relevant data protection statute, or conversely, do something in an attempt to bring them into compliance therewith.

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

There is no specific statutory provision that either allows or prohibits this.

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

Canadian Privacy Statutes do not set out any specific qualifications for the Privacy Officer. In a guidance document entitled *Getting Accountability Right with a Privacy Management Program* (hereinafter, “*Getting Accountability Right*”), the Federal, British Columbia and Alberta privacy regulators set out what the role of the Privacy Officer should entail, and their expectation that he or she be supported by proper training, resources and staff. Practically, a Privacy Officer would be expected to have a broad-based skill set, particularly with respect to compliance and risk management, as well as familiarity with the legal and regulatory frameworks under Canadian Privacy Statutes.

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

At law, a Privacy Officer is generally responsible for ensuring the organisation’s compliance with the applicable privacy statute.

In *Getting Accountability Right*, the Federal, British Columbia and Alberta privacy regulatory authorities describe the role of the Privacy Officer more specifically as the individual who is accountable for structuring, designing and managing the programme, including all procedures, training, monitoring/auditing, documentation, evaluation, and follow-up. Depending on the type and size of the organisation, these Canadian privacy regulatory authorities expect the Privacy Officer to, among other things: establish and implement programme controls, in coordination with other appropriate persons responsible for related functions within the organisation; be responsible for the ongoing assessment and revision of programme controls; represent the organisation in the event of a complaint investigation by a Privacy Commissioner’s office; and most critically, advocate privacy protection within the organisation itself.

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

There is no requirement to register or notify the Data Protection Officer with the relevant data protection authorities.

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

Organisations must be open about, and make available in a form that is generally understandable, the contact information of the person who is accountable for the organisation’s policies and practices and to whom complaints or inquiries can be made. Canadian privacy regulatory authorities expect the Privacy Officer’s contact information to be included in a public-facing privacy policy.

## 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, under PIPEDA, an organisation is required to “use contractual or other means to provide a comparable level of protection while the information is being processed by a third party”. The failure to have appropriate confidentiality agreements in place with third-party contractors has been found to be a breach of the accountability principle.

#### 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.)?

In the private sector context, Canadian Privacy Statutes do not specify the requirements to be included in agreements with third-party processors. However, some privacy laws, and their accompanying regulations, in the health sector for instance, more expressly set out the terms and conditions to be included in written agreements between institutions and information managers. (*See, for example, section 66 of Alberta’s Health Information Act, R.S.A. 2000, c. H-5, and accompanying Regulation 70/2001.*)

## 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 email and SMS text messages is subject to both the requirements under Canadian Privacy Statutes and Canada’s anti-spam legislation (“CASL”). In general, under CASL, it is a violation to send, or cause or permit to be sent, a commercial electronic message (defined broadly to include text, sound, voice or image messages) to an electronic address unless the recipient has provided express or implied consent (as defined in the Act) and the message complies with the prescribed form and content requirements, including an unsubscribe mechanism.

#### 9.2 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 marketing in Canada is subject to the requirements of Canadian Privacy Statutes as well as the Canadian Radio-Television and Telecommunications Commission’s (“CRTC”) Unsolicited Telecommunications Rules. These rules include specific requirements related to the National Do-Not-Call List (“National DNCL”), telemarketing and the use of automatic dialling-announcing devices.

Under Canada's Do-Not-Call List Rules ("DNCL Rules"), an individual may register their telephone or fax number on the National DNCL to indicate that they do not wish to receive unsolicited telemarketing communications. In general, organisations are prohibited from placing unsolicited telemarketing calls (telephone or fax) to numbers registered on the National DNCL unless express consent has been obtained directly from the individual in the manner prescribed under the DNCL Rules. Under the CRTC Telemarketing Rules, an organisation must maintain its own internal Do-Not-Call List and must not initiate telemarketing telecommunications to an individual on its own list.

Postal marketing communications are not specifically regulated, but must comply with the requirements of Canadian Privacy Statutes.

---

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

---

Yes, they do apply.

---

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

---

Yes. The Canadian privacy regulatory authorities have issued multiple reports of findings related to secondary marketing practices. The CRTC is also active in enforcing the Unsolicited Telecommunications Rules.

Canada's anti-spam legislation ("CASL") came into force on July 1, 2014. The CRTC has been actively enforcing CASL and has completed dozens of investigations over the past three years.

---

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

---

It is only lawful if the individuals on the list were clearly and accurately informed at the point of collection about how their addresses would be used and if they consented to having their email addresses collected and used for marketing purposes. In addition, they must be able to opt-out of receiving messages at any time in the future.

---

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

---

Under Canadian Privacy Statutes, there are no specific penalties related to the unlawful sending of marketing communications. However, organisations may be subject to a complaint and investigation. In Alberta, British Columbia and Québec, an investigation may be elevated to a formal inquiry resulting in an order. Failure to comply with an order can result in fines of up to \$100,000 in Alberta and British Columbia. In Alberta and Québec, organisations can also be subject to fines for failure to comply with the relevant requirements of the Acts of up to \$100,000 in Alberta and \$10,000 in Québec for a first offence and \$20,000 for a subsequent offence.

The CRTC has the legislative authority under the *Telecommunications Act* to impose administrative monetary penalties for violation of the Unsolicited Telecommunications Rules. The maximum administrative monetary penalty for each violation of the Unsolicited Telecommunications Rules is \$15,000 for a corporation. A violation that continues for more than one day constitutes a separate violation for each day that it is continued. In addition,

a person that contravenes any prohibition or requirement of the Commission related to the Unsolicited Telecommunications Rules may be guilty of an offence punishable on summary conviction and liable, in the case of a corporation, to a fine not exceeding \$100,000 for a first offence or \$250,000 for a subsequent offence. There is also a limited private right of action that allows a person to sue for damages that result from any act or omission that is contrary to the *Telecommunications Act* or a decision or regulations.

The CRTC is also the agency primarily responsible for regulatory enforcement of CASL's commercial electronic message provisions. CASL permits the CRTC to impose administrative monetary penalties of up to \$1 million per violation for individuals and \$10 million for businesses. CASL outlines a range of factors to be considered in assessing the penalty amount, including the nature and scope of the violation. CASL also sets forth a private right of action permitting individuals to bring a civil action for alleged violations of CASL (\$200 for each contravention up to a maximum of \$1 million each day for a violation of the provisions addressing unsolicited electronic messages).

---

## 10 Cookies

---



---

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

---

There are no specific restrictions with respect to cookies under Canadian Privacy Statutes. As with other forms of collection, use and disclosure of personal information in the course of commercial activities, cookies are subject to the general requirements of Canadian Privacy Statutes.

Under Canadian Privacy Statutes, implied consent can be relied upon for the collection and use of personal information through cookies to the extent that the personal information involved is non-sensitive in nature and that it accords with the reasonable expectations of individuals.

The Privacy Commissioner of Canada's regulatory guidance on *Online Behavioural Advertising* affirmed that implied (or opt-out) consent is reasonable for the purposes of online behavioural advertising provided that:

- individuals are made aware of the purposes for the practice in a manner that is clear and understandable;
- individuals are informed of these purposes at or before the time of collection and provided with information about the various parties involved in online behavioural advertising;
- individuals are able to easily opt-out of the practice at or before the time the information is collected;
- the opt-out takes effect immediately and is persistent;
- the information collected and used is limited, to the extent practicable, to non-sensitive information; and
- information collected and used is destroyed as soon as possible or effectively de-identified.

If, however, the personal information collected and used is sensitive in nature, express consent is required.

---

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

---

Although there are no explicit legislative restrictions with respect to cookies specifically, the Office of the Privacy Commissioner of Canada ("OPC") has restricted the following uses:



The first is in respect of zombie cookies, supercookies, third-party cookies that appear to be first-party cookies, device fingerprinting and other techniques that cannot be controlled by individuals. Where a tracking technique offers no option for user control, and therefore no ability for an individual to consent or withdraw consent to the collection of their personal information for online behavioural advertising purposes, the OPC's position is that that such tracking should not be undertaken because it cannot be done in compliance with PIPEDA.

Secondly, given the practical obstacles to obtaining meaningful consent from children, the OPC's position is that organisations should avoid knowingly tracking children and tracking on websites aimed at children. The OPC takes the view that in all but exceptional cases, consent for the collection, use and disclosure of personal information of children under the age of 13 must be obtained from their parents or guardians. Youth between 13 years and the applicable age of majority can give meaningful consent, provided the organisation's consent process reasonably takes into account their level of maturity and is adapted accordingly.

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

Yes. The OPC has issued several reports of findings in cases involving cookies in the context of online behavioural advertising. As examples, one case involved sensitive health information (PIPEDA Report of Findings #2014-001), and the other involved a website aimed at children (PIPEDA Report of Findings #2014-011).

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

Under Canadian Privacy Statutes, there are no specific penalties related to cookie restrictions. However, organisations may be subject to a complaint and investigation under Canadian Privacy Statutes. In Alberta and British Columbia, an investigation may be elevated to a formal inquiry resulting in an order. Failure to comply with an order can result in fines of up to \$100,000. In Alberta and Québec, organisations can also be subject to fines for failure to comply with the relevant requirements of the Acts of up to \$100,000 in Alberta and \$10,000 in Québec for a first offence and \$20,000 for a subsequent offence.

## **11 Restrictions on International Data Transfers**

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

Under Canadian Privacy Statutes governing the private sector, organisations are responsible for personal information in their custody or control, including personal information transferred to third parties for processing. In general, Canadian Privacy Statutes permit the non-consensual transfer of personal information to third-party processors outside Canada, provided the transferring organisation uses contractual or other means to provide a comparable level of protection while the information is being processed by the foreign processor.

In Alberta, more specifically, if an organisation uses a service provider outside Canada to collect, use, disclose or store personal information, the organisation must specify, in its privacy policies

and practices, the foreign jurisdictions in which the collection, use, disclosure or storage is taking place, and the purposes for which the foreign service provider has been authorised to collect, use or disclose personal information on its behalf.

### **11.2 Please describe the mechanisms companies 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, companies enter into an agreement when transferring data outside of Canada for processing purposes to ensure that the data transferred is afforded a comparable level of protection to that under Canadian Privacy Statutes. Depending on the size and the context of the data transfer arrangement in question, there are a number of measures that companies take to establish an appropriate vendor management framework, including: (i) due diligence, in particular with respect to security safeguards; (ii) contractual arrangements setting out requisite controls and conditions; (iii) appropriate notice to employees or consumers; and (iv) appropriate monitoring of the service provider arrangement. While consent *per se* is not required, notification is.

### **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.**

Transfers of personal data to other jurisdictions do not require registration/notification or prior approval from the relevant data protection authorities.

## **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.)?**

Under Canadian Privacy Statutes, a whistle-blower who has reasonable grounds to believe that a provision of the relevant statute has been, or will be, contravened may notify the data protection authority and request that their identity be kept confidential. The data protection authority shall keep confidential the person's identity and the information he or she relayed, accordingly.

The statutes further prohibit employers from taking retaliatory action against an employee who, acting in good faith and on the basis of reasonable belief, disclosed such information to the data protection authority. Any employer who knowingly contravenes this prohibition is guilty of an offence and may be subject to a fine.

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

Anonymous reporting is not prohibited or discouraged under Canadian Privacy Statutes. As a matter of practice, anonymous

reporting of facts that are credible and can be independently verified may proceed as a Commissioner-initiated complaint if there are reasonable grounds to believe that an investigation is warranted.

## 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 does not require separate registration/notification or prior approval from the relevant data protection authorities. However, as a best practice in some jurisdictions, and as a matter of policy in others, organisations must conduct a privacy impact assessment and seek input from the relevant data protection authority before introducing the use of CCTV.

Appropriate and clear notice should be provided to individuals prior to the collection of personal information through video surveillance. This notice should include the purposes of the video surveillance and contact information in case the individual has questions or wishes to request access to their images.

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

The use of CCTV must only be for purposes that a reasonable person would consider to be appropriate in the circumstances. For instance, the use of CCTV to ensure the protection of company assets that have come under threat of being damaged or stolen, or the safety of customers in situations that have proven to be demonstrably dangerous may be considered reasonable. On the other hand, using CCTV to generally monitor employee performance in the absence of any prior concerns having been raised or any suspected wrongdoing may not be.

## 14 Employee Monitoring

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

Employee monitoring would be permissible (both in the workplace and otherwise), provided that it is conducted in conformity with the principles under Canadian Privacy Statutes.

In particular, the monitoring must be conducted for a purpose consistent with what a reasonable person would consider appropriate in the circumstances. Canadian privacy regulatory authorities generally use a four-part test to assist in determining the reasonableness of employee monitoring:

- Is the surveillance demonstrably necessary to meet a specific need?
- Is the measure likely to be effective in meeting that need?
- Is the loss of privacy proportional to the benefit gained?
- Is there a less privacy-invasive way that the employer could achieve the same end?

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

Canadian privacy statutes governing the private sector generally

allow for the collection, use and disclosure of employee personal information without consent if it is solely for the purposes reasonably required to establish, manage or terminate an employment relationship between the organisation and that individual.

While the statutes allow for the collection of personal information without consent, within the bounds of reasonableness, they nonetheless require the employer to be transparent about it; accordingly, organisations must notify employees that it is occurring, and explain the purpose(s) for the collection (such as employee safety).

Employers typically provide notice about video surveillance or monitoring upon entry to the workplace area under surveillance or upon use of the technology being monitored. Employers also implement video surveillance and monitoring policies and reference such activities in relevant privacy statements.

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

There is no express requirement to notify trade unions regarding the use of employee monitoring under Canadian Privacy Statutes.

## 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.)?

Canadian Privacy Statutes contain specific provisions relating to the safeguarding of personal information. In essence, these provisions require organisations to implement reasonable technical, physical and administrative measures to protect personal information against loss or theft, as well as unauthorised access, disclosure, copying, use, modification or destruction. The security safeguards must be appropriate to the sensitivity of the information, such that, the more sensitive the information, the higher the level of protection that will be required.

An organisation is responsible for protecting personal information in its possession or custody, including information that has been transferred to a third party for processing. They must ensure a comparable level of protection through contractual or other means.

### 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) expects voluntary breach reporting.

The Federal private sector privacy law, PIPEDA, was amended in 2015 to include new breach notification requirements that will come into force November 1, 2018. Once these provisions are in force, PIPEDA will require organisations to report to the Privacy Commissioner any breach of security safeguards involving personal information under its control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual. The report must be made in prescribed form and manner and provided as soon as feasible after the organisation determines that the breach has occurred. Reports to the Commissioner must include the following:

- a. a description of the circumstances of the breach and, if known, the cause;
- b. the day on which, or the period during which, the breach occurred or, if neither is known, the approximate period;
- c. a description of the personal information that is the subject of the breach to the extent that the information is known;
- d. the number of individuals affected by the breach or, if unknown, the approximate number;
- e. a description of the steps that the organisation has taken to reduce the risk of harm to affected individuals that could result from the breach or to mitigate that harm;
- f. a description of the steps that the organisation has taken or intends to take to notify affected individuals of the breach; and
- g. the name and contact information of a person who can answer, on behalf of the organisation, the Commissioner's questions about the breach.

Moreover, the new breach provisions in PIPEDA will require organisations to keep records, in prescribed form, of every breach of security safeguards involving personal information under its control, and to provide the Commissioner with a copy of such records on request.

Under PIPA Alberta, an organisation is required to provide notice to the Commissioner without unreasonable delay of a breach where there is a real risk of significant harm to individuals. Notice to the Commissioner must be in writing and include similar details as those that will be required under PIPEDA (above).

**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) expects voluntary breach reporting.**

As of November 1, 2018, PIPEDA's breach notification provisions will require an organisation to notify affected individuals of a breach of security safeguards if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual. The notification must be given as soon as feasible after the organisation determines that the breach has occurred. It must be conspicuous and given directly to the individual in the manner prescribed by the regulations. Indirect notification is also permissible in circumstances where direct notification is likely to cause further harm to the affected individual or undue hardship for the organisation, or where the organisation does not have contact information for the affected individual.

The contents of the notification to individuals will have to include:

- a. a description of the circumstances of the breach;
- b. the day on which, or period during which, the breach occurred or, if neither is known, the approximate period;
- c. a description of the personal information that is the subject of the breach to the extent that the information is known;
- d. a description of the steps that the organisation has taken to reduce the risk of harm that could result from the breach;

- e. a description of the steps that affected individuals could take to reduce the risk of harm that could result from the breach or to mitigate that harm; and
- f. contact information that the affected individual can use to obtain further information about the breach.

Under PIPEDA, when notice is given to individuals, it must also be given to any other organisation or government institution if the notifying organisation believes that the other organisation or the government institution may be able to reduce the risk of harm or mitigate that harm.

Under PIPA Alberta, the Commissioner, once notified, may subsequently require organisations to notify affected individuals directly of the loss or unauthorised disclosure, unless the Commissioner determines that direct notification would be unreasonable in the circumstances. Such notification must include certain elements which are similar to those that will be required under PIPEDA (above).

While other data protection statutes do not contain any express data breach notification requirements, Commissioners' findings and other guidance documents suggest that a duty to notify affected individuals is an implicit part of the general safeguarding requirements in circumstances where material harm is reasonably foreseeable, and such notification would serve to protect personal information from further unauthorised access, use or disclosure.

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

Under PIPEDA, failure to comply with the breach notification provisions will (as of November 1, 2018) be an offence under the Act punishable on summary conviction liable to a fine not exceeding \$10,000, or as an indictable offence liable to a fine not exceeding \$100,000.

Under PIPA Alberta, a failure to notify the Commissioner in the event of a breach is an offence. A person who commits an offence is liable, in the case of an individual, to a fine not exceeding \$10,000, and in the case of a person other than an individual, to a fine not exceeding \$100,000.

## 16 Enforcement and Sanctions

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

**Powers of Investigation**

Under PIPEDA, the Federal Privacy Commissioner shall investigate a complaint made by an individual, subject to a discretion to decline or discontinue complaints in certain circumstances.

The Federal Privacy Commissioner can also initiate an investigation based on reasonable grounds to believe that a matter warrants it.

In the course of an investigation, the Commissioner has substantial powers, including the power to summon witnesses to give oral or written evidence, inspect documents and/or compel the production thereof, and inspect premises other than a dwelling house.

Under PIPA Alberta and PIPA BC, the Commissioners have similar powers of investigation. However, where a matter is not otherwise resolved, an investigation may be elevated to a formal inquiry.

**Powers of Enforcement**

Upon concluding an investigation under PIPEDA, the Privacy Commissioner issues a report of findings and, if applicable, recommendations for compliance. Although the report is non-binding in nature, it may be made public at the discretion of the Privacy Commissioner if it is in the public interest.

The complainant or the Commissioner, with the individual's consent, may apply to the Federal Court for a *de novo* hearing. The Court has broad remedial powers to order correction of the organisation's practices and award damages to the complainant, including damages for any "humiliation" suffered.

The OPC and the organisation may agree to enter into a voluntary compliance agreement whereby the organisation undertakes to comply with the recommendations made and bring itself into compliance with PIPEDA.

When a compliance agreement is entered into, the Commissioner shall not apply to the Court for a hearing or shall suspend any pending court application, unless or until there is breach of the agreement. If an organisation fails to live up to its commitments in a compliance agreement, the OPC could, after notifying the organisation, apply to the Court for an order requiring the organisation to comply with the terms of the agreement.

In Alberta and British Columbia, an inquiry may result in an enforceable order. Organisations are required to comply with the order within a prescribed time period, unless they apply for judicial review. In Alberta, the order may be filed with the Court and becomes enforceable as a judgment. Once an order is final, an affected individual has a cause of action against the organisation for damages for loss or injury that the individual has suffered as a result of the breach.

Similarly, in Québec, an order must be obeyed within a prescribed time period. An individual may appeal to the judge of the Court of Québec on questions of law or jurisdiction with respect to a final decision.

**Audits**

The OPC and the OIPC BC have the express authority to audit the personal information practices of an organisation upon reasonable grounds that the organisation is contravening the Act. The results of the audit are made public.

**Offences / Criminal Sanctions**

In Québec, Alberta and British Columbia, there are certain statutory provisions which, if violated, could constitute an offence and result in fines of up to \$10,000 for a first offence and \$20,000 for a subsequent offence in Québec, and \$100,000 for an offence in Alberta and British Columbia. This includes the offence of failing to comply with an order made by the Commissioner.

Under PIPEDA, there are more limited statutory provisions, the contravention of which may result in criminal sanctions. For example, any person who knowingly destroys personal information that is the subject of an access to personal information request, retaliates against a whistle-blowing employee, obstructs the Commissioner in the course of a complaint investigation, uses deception or coercion to collect personal information in contravention of the Act, or (as of November 1, 2018) fails to notify in the event of a breach, is guilty of an offence and liable to a fine of \$10,000 for an offence punishable on summary conviction or \$100,000 for an indictable offence.

**Data-Sharing Arrangements**

The Privacy Commissioner of Canada has the express authority under PIPEDA to enter into data-sharing arrangements with provincial or foreign counterparts, as considered appropriate, to coordinate their Office's activities, (including investigations) and ensure that personal information is protected in as consistent a manner as possible.

## 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?

To the extent that data protection authorities have the power to issue binding orders (*see above*), they can ban a particular processing activity or apply to the Court for an enforceable order to that effect.

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

Canada has one of the most active privacy regulatory enforcement arenas in the world. The OPC and the provincial privacy regulatory authorities in the provinces of Alberta and British Columbia have been actively focused on early resolving individual complaints

wherever possible, in order to redirect limited resources to the investigation of novel, precedent-setting complaints that raise large, systemic issues particularly in the online world (including complaints against companies such as Facebook and Google).

There has also been an increasing trend of Canadian privacy regulatory authorities initiating investigations of their own accord. The OPC, in particular, is adopting a deliberate strategy of proactive enforcement through formal, Commissioner-initiated investigations, as well as active participation in the less formal, online privacy sweeps of the Global Privacy Enforcement Network ("GPEN").

The OPC is also collaborating more frequently with its national and international counterparts, to conduct joint investigations in accordance with formal written arrangements (e.g., Ashley Madison and WhatsApp).

Canadian privacy regulators actively pursue softer compliance tools as well, such as guideline development, public education and research on a range of emerging privacy issues – both individually and jointly – to encourage compliance up front before problems arise.

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

Although PIPEDA is silent with respect to its territorial reach, the Federal Court of Canada has found that PIPEDA will apply to businesses established in other jurisdictions if there is a "real and substantial connection" between the organisation's activities and Canada. For instance, with respect to websites, the relevant connecting factors include: (1) where promotional efforts are being targeted; (2) the location of end-users; (3) the source of the content on the website; (4) the location of the website operator; and (5) the location of the host server.

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

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

Although the language varies across the statutes, under Canadian Privacy Statutes, there is generally an exception to the consent requirement when disclosing information (i) to comply with the rules of court relating to the production of records, and (ii) where required by law.

When disclosing personal information in either of these contexts, the remaining requirements under Canadian Privacy Statutes still apply. As such, organisations must only disclose the personal information in the manner and to the extent to which a reasonable person would consider appropriate in the circumstances, must limit the amount of personal information that is disclosed to that which is reasonably necessary in the circumstances, and must appropriately safeguard the transmission of personal information.

The OPC also expects organisations to be open and transparent when transferring data across borders, in particular by openly notifying individuals that personal information transferred to another jurisdiction becomes subject to foreign laws and may be accessed by the courts, law enforcement and national security authorities in those jurisdictions.



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

The OPC has released a guidance document entitled *Guidelines for Processing Personal Data Across Borders* which addresses lawful access by foreign authorities.

The OPC has also released a guidance document entitled *PIPEDA and Your Practice: A Privacy Handbook for Lawyers* which addresses privacy issues associated with e-discovery.

## 18 Trends and Developments

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

See above a description of the more proactive enforcement trends that have emerged during recent years, including the previous 12 months.

In terms of relevant case law, courts continue to refine the contours of common law privacy torts, including the tort of invasion of privacy and the tort of publication of embarrassing private facts.

Also, the Supreme Court of Canada has over the past year rendered two important decisions: one on the validity of the forum selection clause used by Facebook in its terms of use (*Douez v. Facebook Inc.*, 2017 SCC 33); and the other on the validity of a British Columbia court-ordered injunction against Google to globally de-index websites of a certain distributor who was continuing to act unlawfully (*Google Inc. v. Equustek Solutions Inc.*, 2017 SCC 34).

This coming year, in a case called *R. v. Jarvis*, the Supreme Court of Canada will be asked to define the concept of reasonable expectation of privacy in public places for the purpose of enforcing voyeurism provisions of the Criminal Code of Canada.

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

Canada’s Federal Privacy regulator, the OPC, has established four strategic privacy priorities to guide the Office’s discretionary work through 2020: economics of personal information; government surveillance; reputation and privacy; and the body as information.

The Office is currently focused on implementing its recommendations for enhanced consent under PIPEDA, including by finalising its online consent guidance this year, among other related guidance documents it intends to publish both for organisations and individuals in the short to medium term, including on de-identification.

The OPC continues to focus on national security reforms in Canada and the interplay with data protection. The Office also intends to finalise its policy position on the right to be forgotten in Canada and continues to shift its focus towards more proactive enforcement of broad systemic issues in collaboration with its national and international counterparts.

Canadian privacy regulators are increasingly interested in the role that ethics should play in the effective governance of big data, analytics and artificial intelligence initiatives. There is also an active interest on the part of Canadian regulators to pursue the growing intersection between data protection, competition and consumer protection law, and a recognition of the corresponding need for increased collaboration between them.

The CRTC continues to actively enforce the commercial electronic message provisions in CASL. The CRTC has entered into five undertakings regarding potential CASL violations that included payments to the CRTC ranging from \$10,000 to \$200,000, and has made three compliance and enforcement decisions with administrative monetary penalties ranging from \$15,000 to \$200,000.

**Adam Kardash**

Osler, Hoskin & Harcourt LLP  
100 King Street West  
1 First Canadian Place  
Suite 6200, P.O. Box 50  
Toronto ON M5X 1B8  
Canada

Tel: +1 416 862 4703  
Email: [akardash@osler.com](mailto:akardash@osler.com)  
URL: [www.osler.com](http://www.osler.com)

Adam is an acknowledged Canadian legal industry leader in privacy and data management; he co-leads Osler's national Privacy and Data Management Group. Adam has been lead counsel on many of the most significant privacy matters in Canada. He advises Fortune 500 clients in their business-critical data protection issues, compliance initiatives and data governance. He regularly represents clients on regulatory investigations and security breaches.

Adam is Special Counsel to the Interactive Advertising Bureau of Canada and Counsel to the Digital Advertising Alliance of Canada. He has extensive experience in the privacy law area and regularly advises Chief Privacy Officers, in-house counsel and compliance professionals in the private, health, public and not-for-profit sectors on managing security incidents, privacy regulatory investigations, anti-spam law compliance, privacy and security reviews/audits, privacy policies, practices and procedures, privacy compliance initiatives, and service provider arrangements involving personal information, including trans-border data flows.

For further information, please visit <https://www.osler.com/en/team/adam-kardash>.

**Patricia Kosseim**

Osler, Hoskin & Harcourt LLP  
Suite 1900  
340 Albert Street  
Ottawa ON K1R 7Y6  
Canada

Tel: +1 613 787 1008  
Email: [pkosseim@osler.com](mailto:pkosseim@osler.com)  
URL: [www.osler.com](http://www.osler.com)

Patricia is Counsel in Osler's Privacy and Data Management Group and Co-Leader of Osler's AccessPrivacy® platform. Patricia is a national leading expert in privacy and access law, having served over a decade as Senior General Counsel at the Office of the Privacy Commissioner of Canada (OPC). There she provided strategic legal and policy advice on complex privacy issues; advised Parliament on privacy implications of legislative bills; led research initiatives on emerging information technologies; and advanced privacy law in major litigation cases before the courts, including the Supreme Court of Canada.

Previously, Patricia worked at Genome Canada and the Canadian Institutes of Health Research, where she developed and led national strategies for addressing legal, ethical and social implications of science and technology. Patricia began her career in Montreal practising in the areas of health law, privacy law, civil litigation, and labour and employment with another leading national law firm. She has published and spoken extensively on matters of privacy law, health law and ethics.

For further information, please visit <https://www.osler.com/en/team/patricia-kosseim>.

# OSLER

Osler, Hoskin  
& Harcourt LLP

Osler is a leading business law firm advising Canadian and international clients from offices across Canada and in New York. With well over 400 lawyers, the firm is recognised for the breadth and depth of its practice and is consistently ranked as one of Canada's top firms in national and international surveys. Osler has the largest team of practitioners who focus exclusively on privacy and data management in Canada, providing expert legal advice on increasingly complex issues.

Osler's AccessPrivacy® provides an integrated suite of innovative information solutions, consulting services and thought leadership. The AccessPrivacy® platform helps organisations in the public, private and not-for-profit sectors navigate the complex regulatory environment and develop a strategic approach to privacy and information management, supported by sound policies and practices.

# Chile

Rossi Asociados

Claudia Rossi



## 1 Relevant Legislation and Competent Authorities

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

The principal data protection legislation is Law 19.628 on the protection of personal life (also referred to herein as the Law).

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

Yes. The Chilean Constitution, in its Article 19 Nos. 4 and 5, sets forth and guarantees the right of privacy. Also, the Consumer Protection Law (Law 19.496) establishes rules on unsolicited commercial or marketing communications sent to consumers.

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

Yes. Health, labour, telecommunications, financial, banking and commercial laws impact data protection.

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

There is not a data protection authority established by law. This means that the enforcement of the law is delivered to the courts of justice and every affected subject enforces their rights individually. Regarding transparency, the Chilean Transparency Council is an authority created by the Law on Transparency of Public Functions and Access to Information of State Administration, whose main task is to ensure proper compliance of this law, which was enacted on August 20<sup>th</sup>, 2008.

## 2 Definitions

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

- **“Processing”**: any operation or complex set of operations or technical processes, automated or not, that allows the collecting, storing, recording, organising, devising, selecting, extracting, confronting, interconnecting, dissociating, communicating, assigning, transferring, or cancelling of personal data, or the use of it in any other way.
- **“Controller”**: this is not applicable.
- **“Processor”**: the natural person or legal private entity, or the respective public body, which is responsible for making decisions related to personal data processing.
- **“Data Subject”**: the individual to whom the personal data refers.
- **“Sensitive Personal Data”**: personal data referring to individuals’ physical or moral characteristics or to facts or circumstances of their private life or intimacy, such as personal habits, racial origin, ideologies and political opinions, religious beliefs or convictions, physical or mental health, and sexual life.
- **“Data Breach”**: the Law does not give a definition for this concept.
- *Other key definitions – please specify (e.g., “Pseudonymous Data”, “Direct Personal Data”, “Indirect Personal Data”)*
  - **“Database Responsible”** (which the Law named as: “Responsible for the Registry or Data Bank”, equal or similar to “Controller”): the natural person or private legal person, or the respective public entity, which is responsible for decisions related to the processing of personal data.
  - **“Obsolete Data”**: that which has lost its relevance by law by means of the fulfilment of the condition or the expiration of the term set forth for its validity or, in the absence of any specific law regulating this, the change of facts or circumstances covered by it.
  - **“Statistical Data”**: the data that, in its origin or as a result of its processing, cannot be associated with an identified or identifiable subject.
  - **“Sources Accessible to the Public”**: the personal data registers or recomputations, public or private, whose access is not restricted or reserved to solicitors.
  - **“Registry or Data Bank”**: the organised set of personal data, automated or not, and its form or the method of its creation or organisation, that allows for the comparison of data, as well as to facilitate data processing.
  - **“Data Disassociation Procedure”**: all processing of personal data so that the information obtained cannot be associated with a person determined or determinable.

### 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 does not contain rules for data processing outside of the country. Further, Article 5 of the Law specifically determines that its provisions do not apply to data transmitted to international organisations in compliance with international treaties or agreements in force.

### 4 Key Principles

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

- **Transparency**  
The person authorising must be properly informed about the purpose of the storage of its personal data and its possible communication to the public.
- **Lawful basis for processing**  
According to Article 4 of the Law, personal data processing requires explicit authorisation, either as provided by law, or by way of consent from the data subject.
- **Purpose limitation**  
Personal Data shall be used only for the purpose for which they were collected unless they are obtained from open registers or public sources. This principle is established in Article 9 of the Law.
- **Data minimisation**  
This is not applicable.
- **Proportionality**  
This is not applicable.
- **Retention**  
This is not applicable.
- *Other key principles – please specify*  
There are no other specific key 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**  
The data subject has the right to request to the person responsible for any private or public data bank details on the information of his or her personal data being held, its source, the purpose of collection and the name of the entities to which its data is being transmitted. There is no right to obtain copies of data by the data subject.
- **Right to rectification of errors**  
The personal data must be modified when they are inaccurate, incomplete, misleading or outdated.
- **Right to deletion/right to be forgotten**  
Personal data must be deleted or cancelled when its storage has no legal basis or when they have expired. The Law does not contemplate the specific right to be forgotten.

#### ■ **Right to object to processing**

The Law only recognises the right of opposition, which refers to the possibility that the data subject opposes the use or transmission of its personal data. This right applies solely in the following cases:

1. For advertising purposes.
2. For market surveys.
3. For opinion polls.

#### ■ **Right to restrict processing**

The Law does not provide a general right to restrict data processing,

#### ■ **Right to data portability**

This is not applicable.

#### ■ **Right to withdraw consent**

The Law allows data subjects to withdraw their consent, but it must be done in written form and it will not have a retroactive effect.

#### ■ **Right to object to marketing**

As previously mentioned, the Law provides the right of opposition by the data subject regarding the use or transmission of its personal data for: 1) advertising purposes; 2) market surveys; and 3) opinion polls.

#### ■ **Right to complain to the relevant data protection authority(ies)**

This is not applicable.

#### ■ *Other key rights – please specify*

There are no other specific key 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?

There is no legal obligation of this kind.

#### 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.**

This is not applicable.

**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 to 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 Law does not regulate this matter, but it contains some rules for the automated transmission of data. Article 5 provides that the person responsible for the registry or personal database must take care of it with due diligence and is liable for damages. The same entity may establish an automated personal data transmission system, provided that it adequately secures the rights or interests of the parties involved and such transmission is strictly related to the duties and goals of the participating entities.

**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 legal requirement or obligation regarding this. The Law only stipulates that in case of transmission of personal data through an electronic network, the following must be left on record:

1. Identification of the requesting party.
2. Reason and purpose of the inquiry.
3. Type of data transmitted.

## 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 Article 4 of the Law, no authorisation is required from the data subject for the collection of personal data from sources accessible to the public, if such data are necessary for commercial communications of direct answer or direct marketing of goods and services. In this case, personal data can include information such as email addresses, conventional addresses, etc.

In any case, the Consumer Protection Law (Law 19.496) establishes rules on the protection of consumer rights, particularly when referring to unsolicited commercial or marketing communications sent to consumers. Article 28 B of this Law regulates unsolicited commercial or marketing communications sent via email to consumers, specifying, among other things, that such communication must contain a valid email address to which the recipient can request the suspension of further communications, otherwise referred to as an opt-out system. From the moment that the recipient requests the suspension of sending further emails, any communication or unsolicited email is forbidden by law.

### 9.2 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 same Article 28 B of the Consumer Protection Law establishes that providers that send promotional or advertising communications to consumers by means of postal mail, fax, calls or services phone messaging must indicate an expedited way in which recipients may request the suspension of them. Once the suspension is requested, the sending of new communications will be prohibited. Notably, there is an app called “do not bother” (*no molestar*), which was released in 2013 by the National Consumer Service (Sernac) as an initiative consisting of a list or register in which users who do not want to receive calls from companies can be enrolled. The National Consumer Service (Sernac) notifies the companies that make calls to the list of users who do not give their consent to receive advertising or marketing communications.

### 9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

This is not applicable.

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

This is not applicable.

### 9.5 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 regulation regarding this.

### 9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

The National Consumer Service (Sernac) can adopt all appropriate actions to ensure that the rights of consumers are respected with regards to marketing communications, from legal actions to economic sanctions. According to Article 24 of the Consumer Protection Law, a fine of up to 50 monthly tax units (UTM) will apply in cases of this type of infringement (UTM is the acronym for the Spanish Unidad Tributaria Mensual, or Monthly Tax Unit, a unit of account used in Chile for tax purposes and calculated and published by the Chilean Central Bank. 50 UTM equals approx. USD 3,800).

## 10 Cookies

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

There is no legislation in Chile that regulates this topic.

### 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?

This is not applicable.

### 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 Law does not regulate cross-border transfer of personal data. Therefore, Chile is not considered as a “safe harbour” for personal data purposes.

However, the Law contains some rules for the automated transmission of data. Article 5 of the Law prescribes that the person responsible for a registry or database may establish an automated personal data transmission system, provided that it adequately secures the rights or interests of the parties involved, and such transmission is strictly related to the duties and goals of the participating entities.

Further, in the case of a request for the transmission of personal data through an electronic network, the following shall be put on record:

- Identification of the requesting party.
- Reason and purpose of the inquiry.
- Type of data transmitted.

The admissibility of the request must be examined by the entity responsible for the data collection, but the requesting party is responsible for meeting the requirements. The receiving party is only authorised to use such personal data for the purposes that served as the basis for the transmission. This Article does not apply when personal data are available to the public in general.

**11.2 Please describe the mechanisms companies 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.).**

Since there are no legal transfer restrictions, companies use contractual mechanisms such as the EU Standard contractual clauses, for when Chilean companies receive personal data from any country in the EU.

**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 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.)?**

Chile lacks comprehensive whistle-blower laws or legal provisions to protect whistle-blowers from retaliation in both the public and private sectors.

Chilean corporate liability legislation takes into account the effectiveness of a company's compliance programme when determining corporate liability for a crime that may have been committed during that company's activities, or as a mitigating factor when sentencing. Law 20.393, enacted in 2009, allows corporate liability for a range of offences, including foreign bribery. Corporations can avoid or mitigate liability if they have put in place an offence prevention model in accordance with the provisions of this law. One of the required elements of an offence prevention model is a channel for reporting violations. There are no restrictions regarding personal data of the person who may submit, or to whom a report may concern.

Only the Labour Code workplace harassment provisions provide any kind of recourse for private sector whistle-blowers who suffer retaliation for reporting.

**12.2 Is anonymous reporting prohibited, or strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do companies 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)?**

No, it is not necessary.

**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?**

Employers are entitled to monitor employees' conduct and communications in the workplace only under certain circumstances and in compliance with employees' constitutional rights concerning intimacy, private life or honour.

Therefore, in accordance with administrative and judicial jurisprudence, employee monitoring shall only be carried out with regards to information related to the work and in compliance with the non-discrimination principle, and as long as monitoring is previously communicated to employees. It should be a balance between employers' rights (property right and performance of a private economic activity) and employees' rights.

Even though computers at the workplace are the property of the employer, they can – and mostly do – contain information and personal data of employees. The employer can be prevented from monitoring them because it would be a violation of the employee's privacy, unless monitoring is regulated by internal regulations at the workplace.

Further, employers can restrict the use of the internet and declare as not private certain types of activity or communications, but always allowing for appropriate freedom for the employees.

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

Employee consent is required if some kind of permitted monitoring is agreed on the labour contracts. Notice is always required when regulating monitoring at the workplace.

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

It is not mandatory, but it is highly advisable.

## 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.)?**

There are no security measure standards or requirements for the

protection of data. However, the Law, in its Article 11, specifies the general principle in this matter providing that those responsible for the registries or personal databases must “take care of them with due diligence”, and are liable for damages.

**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) expects voluntary breach reporting.**

There are no legal requirements regarding this, as there is no data protection authority to whom breaches can be reported.

**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) expects voluntary breach reporting.**

This is not applicable.

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

This is not applicable.

## 16 Enforcement and Sanctions

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

Investigatory Powers	Civil/Administrative Sanction	Criminal Sanction
This is not applicable.	This is not applicable.	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?**

This is not applicable since there is no data protection authority.

**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 companies 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 companies 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.**

In November 2017, the Ministry of Interior issued the so-called “Spy Decree” (Supreme Decree N°866), that sought to increase the possibilities of interception of communications and data storage of communications of all Chileans, to which the Police and the Public Ministry have access. It expanded the type of communications that can be intercepted, including all types of electronic communication. In addition, it sought to increase the existing policy of storing the activity records (metadata) of the communications of all users of all telecommunications companies, increasing the storage term (from one to two years), and the type of communications whose registration must be stored. Finally, and after a huge debate about the broad scope of this regulation, the Comptroller General's Office of Chile objected to it.

**18.2 What “hot topics” are currently a focus for the data protection regulator?**

The Data Protection Bill N°11144, of presidential initiative, was introduced in March 2017, and recently consolidated with another Bill that proposed similar modifications to our data protection regulation, contained in Law N°19.628 about the Protection of Privacy.

This Bill had been held in Congress for a while since the Senate, on March 22<sup>nd</sup>, 2017, agreed to make some progress and decided to recast it with another Bill (N°11092-07), which intended similar modifications in the matter of data treatment and its regulation. Finally, in March 14<sup>th</sup> of the present year, both Bills were consolidated.

This Bill represents the biggest review in data protection legislation in our country since 1999 and seeks to increase the level of privacy protection in order to comply with international standards in matters of personal data processing, and to meet the guidelines of the Organisation for Economic Cooperation and Development (OECD), which Chile joined in 2010.

The Bill aims to regulate data treatment and reinforce its protection by making important adjustments to our current data protection regulation, contained in Law N°19.628 about the Protection of Privacy.



The most significant changes that this Bill brings to our legislation are the following:

- In the first place, the Bill sets a new scope for our current data protection Law 19.628.
- It incorporates a number of terms and adjusts others that are already established in the current law. One of the most important additions is the definition and requirements of the data subject's consent and the modifications incorporated to the definition of sensitive data. The current legislation does not contemplate such a specific regulation in this matter.
- It informs every data subject of the ARCO rights (access, rectification, cancellation and opposition) specifying their meaning, content and how to exercise each one of them.
- In relation to the data processing of minors, it strengthens the actual regulation in accordance with the new European directive (GDPR). It incorporates new categories of data such as biometric information and data related to the human biological profile.
- One of the most innovative changes is the creation of a data protection entity called the Agency for the Protection of Personal Data. This organism will be in charge of ensuring compliance with the law along with the supervision and inspection of the data controllers. The faculty to sanction non-compliance with the law will apply for both public and private entities.
- To those who process personal data, it establishes the obligation to inform data subjects about the purpose of the collection of their data.
- It creates a series of rules for data transfer operations both nationally and internationally. The criteria used in this Bill is that the transfer of personal data out of the national borders could be made only if the country with whom the transfer is made has adequate standards of security and quality. These standards are set by the Agency for the Protection of Personal Data.

To sum up, all the amendments and guidelines proposed by this Bill are intended to update and modernise the legal framework regarding data protection and resemble as much as possible the new European Union General Data Protection Regulation (GDPR). This because the GDPR is considered to be the most important change in data privacy regulation in 20 years and is therefore a model to follow.

#### Current Status

Since both Bills were recently consolidated in one project, there have been no further progress in the legislative process and the general discussion of the Bill is taking place in the Senate. So, nothing remains but to wait for the Bill to continue its way through the First Constitutional Process, and finally become our new data protection law.



#### **Claudia Rossi**

Rossi Asociados  
Av. Los Leones 220 Of. 502  
Providencia  
Santiago  
Chile

Tel: +56 2 2946 2223  
Email: [crossi@rossiasociados.cl](mailto:crossi@rossiasociados.cl)  
URL: [www.rossiasociados.cl](http://www.rossiasociados.cl)

Claudia Rossi is the founder and partner of Rossi Asociados.

Ms. Rossi's practice focuses primarily on technology-related transactions, including software licensing, hardware, software and distribution arrangements, technology transfer and outsourcing agreements.

Ms. Rossi has considerable experience representing emerging companies and large corporate clients in a broad array of corporate and commercial issues. She handles a wide variety of matters, including: communications; information technology and intellectual property transactions; data privacy and security counselling; joint marketing; strategic alliances; employment contracts; trade secret and intellectual property protection; and tax planning strategies and collaboration agreements, among others.

Ms. Rossi has received recognitions from *Who's Who Legal* and other publications, where she has been listed as one of the leading practitioners on the Chilean market in Telecommunications, Media and Technology.



Rossi Asociados is a boutique law firm based in Santiago, Chile, providing innovative and relevant legal solutions to Chilean and international clients from a wide array of industries. Our practice focuses primarily on commercial, corporate, civil and taxation law, including IP, IT and Telecommunications.

We counsel many of the leading vendors and largest purchasers of technology-related products and services.

We are devoted to creating outstanding added value for our clients and establishing a long-term relationship with them based on our understanding of their business and needs, providing personalised counselling.

# China

King & Wood Mallesons

Susan Ning



Han Wu



## 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 data protection requirements for network operators.

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

There are civil and criminal legislations that have an impact on data protection. In particular, the *General Rules of the Civil Law* became effective on 1 October 2017, in which Article 111 provides that natural persons' personal data is protected by law. Illegally collecting, using, processing or transferring the personal data of others is not allowed.

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 also specific legislations in sectors of banking, insurance, medical, credit information, telecommunications and automobiles that impact data protection, such as the *Measures for Administration of Population Health Information*, the *Medical Records Administration Measures of Medical Institutions*, 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 *Cybersecurity Law*, 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, 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 Industry and Information Technology 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 Industry and Commerce and its local counterparts are responsible for the supervision and administration of personal information of consumers, pursuant to the *Several Provisions on Regulating the Market Order of Internet Information Services*.

## 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 which 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 the telephone number of the natural person.
- **"Processing"**  
Given that the major legislation CSL only provides definitions for few key terms, 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 "**the 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.

Neither the CSL nor the Standard have defined “Processing”, but it is mentioned in the Standard when discussing entrusted processing.

#### ■ “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 to “Processor”. However, the Standard provides the obligations that data processors should comply with in the case of “entrusted processing” in Section 8.1.

#### ■ “Data Subject”

The CSL does 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 the damage of 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.

#### ■ “Data Breach”

Neither the CSL nor the Standard define “Data Breach”.

#### ■ Other key definitions – please specify (e.g., “Pseudonymous Data”, “Direct Personal Data”, “Indirect Personal Data”)

The Standard also provides definitions to other key terms, which, among others, includes “Anonymisation” and “De-identification”.

Anonymisation, as defined in Section 3.13, means making the data subject unidentifiable through technical processing of personal data, and the processed information cannot be restored. Anonymised personal data is no longer considered as personal data.

De-identification, as defined in Section 3.14, means making the data subject unidentifiable if not combined with other information through the technical processing 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?

Theoretically, yes. 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 endangers CII too.

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.

## 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.

In Section 4e), 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.

#### ■ Lawful basis for processing

Article 41 of the CSL requires 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 force, deceive or inveigle 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 5.4 of the Standard further provides exceptions to the requirement of obtaining consent, where consent is not necessary prior to the collection and use 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.

#### ■ 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 lawful, legitimate, necessary and clear purpose of processing personal data.

#### ■ 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 as 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.

## ■ **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 is similar in essence with 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 there should be a minimum retention period of personal data after the processing purpose is fulfilled.

## ■ **Other key principles – please specify**

Ensuring security principle: 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.

## 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**

Given that only rights to rectification and deletion are stated expressly in the CSL, some of the rights hereby listed are provided by the Standard.

Section 7.4 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.

#### ■ **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 provides similar rules in Section 7.5.

#### ■ **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 violate the laws, administrative regulations or the agreement by and between such operator and him or her.

Apart from the above circumstances, Section 7.6 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. Further, Section 7.8 provides that data subjects shall be provided channels to close his or her account and the relevant personal data shall be deleted/anonymised.

#### ■ **Right to object to processing**

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 7.10 of the Standard, a personal data subject will not be provided with a right to object but a right to appeal when 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.

#### ■ **Right to data portability**

The CSL does not provide explicitly for the right to data portability. According to Section 7.9 of the Standard, the right of data portability is of two kinds: (1) the data controller provides a copy of certain personal data to data subject; and (2) the data controller directly sends the copy to a third party where technically feasible.

The personal data which can be portable are confined into four kinds: 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 his/her personal data. Although it is not explicitly provided in the CSL, Section 7.7 of the Standard provides practical guidelines regarding the revocation and modification of consent under two different scenarios: (1) the withdrawal of consent for refusing to receive commercial advertisements; and (2) the withdrawal of consent for entrusted processing and transfer.

#### ■ **Right to object to marketing**

Section 7.7 of the Standard stipulates that data subjects have the right to not receive commercial advertisements that are based on his or her personal data.

#### ■ **Right to complain to the relevant data protection authority(ies)**

Article 12 of the Provisions on Protecting the Personal Information of Telecommunications and Internet Users (“Provisions”) provides that telecommunications business operators and Internet information service providers shall establish a mechanism for handling the users’ complaints, publish their valid contact details, accept complaints relating to the protection of the personal information of users, and answer the relevant complaints. For reporting to authorities, the CSL only 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**

There are no other specific key rights.

## 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. In particular, network operators shall conduct security assessments on transmitting data abroad. The *Measures for the Security Assessment of Personal Data and Important Data to be Transmitted Abroad* (draft for comment, hereinafter “the Draft”) stipulates in Article 8 that if the data transferred in one year contains personal data of over 500,000 people, or contains data in the areas of nuclear facilities, biochemistry, defence industry, population and health, as well as the data of a large-scale project, marine environment, and sensitive geographic information or other



critical information, or other information that could have an impact on national security, economic impact or public interest, then the network operator shall notify the authorities of the relevant industry regarding the assessments.

**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)?**

It is fairly specific. The *Information Security Technology – Guidelines for Data Cross-Border Transfer Security Assessment* (draft) provides that the notification should include, but not be limited to, the basic information of the subject of the security assessment, the information regarding the conduct of the assessment, the results and the risk point of the assessment, and the suggestion for check and correction. Nonetheless, this document is a national standard which is neither legally compulsory nor effective yet.

**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 law does not provide explicitly on this issue. According to the Draft, the notification is made on an annual basis by each network operator that satisfies the conditions mentioned in 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 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)?**

Currently, there is no legislation expressly stating the information that must be included in the notification. Please see question 6.2 regarding the information recommended to be included in the notification.

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

The law does not specify the sanctions for average network operators, but 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 100,000.

**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)?**

Article 8 of the Draft provides that networks operators concerning international data transfer shall conduct a security assessment annually, and make notifications accordingly where required.

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

For CII operators, yes. Article 11 of the Draft provides that CII operators are required to store their data collected and generated in China domestically. Where there are business needs to transfer such data overseas, prior approval from competent authorities of the relevant industry is needed.

**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. It is provided in Article 20 of the Provision 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?**

Currently, there is no specific time frame for the notification. 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 appointments of such officers are mandatory. And Section 10.1 of the Standard specifies that personal data controller shall appoint a Data Protection Officer and set up a Data Protection Department.

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

Since 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 CII operator, a security management officer too, 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 consequential severe 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 consequential severe damage. A fine ranging from RMB10,000 to RMB100,000 may be imposed on the person directly in charge.

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

If a Data Protection Officer failed to perform his or her duty with due diligence, then he or she may be accused of criminal liabilities in respect to 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 does 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.

Currently, there is no specific qualification for the Data Protection Officer required by law.

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

Section 10.1 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 to be directly responsible for the personal data security;
- 2) drafting, issuing, implementing and regularly updating the privacy policy and related regulations;
- 3) 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;
- 4) conducting a personal data security impact assessment;
- 5) organising a personal data security training;
- 6) conducting product or service testing before its release in case of unknown collection, use, sharing and other processing activities of personal data; and
- 7) conducting safety audits.

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

Currently, the law does not require the appointment of a Data Protection Officer to be registered or notified to the relevant data protection authorities.

## 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, there is the requirement to provide a person to contact for the public for the purpose of dealing with users' queries and complaints regarding privacy and data protection issues.

# 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 law does not have such requirement, but Article 8.1 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.

## 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 8.1 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 re-assign a processor, the assistance it shall provide the data controller with, 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 13 of the *Administration of Internet Electronic Mail Services Procedures* provides that the word "advertisement" or "AD" must be indicated in the email subject. 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 electronic mails, including the email address of the sender, and shall ensure that such contact details are valid within 30 days.

Further, under Section 7.7 of the Standard, for advertising in electronic or other forms using personal data, the consent of relevant data subject must be obtained. If the data subject revokes his or her consent for data processing, the data controller shall not continue sending such advertisement.

---

**9.2 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.)**

---

Pursuant to Article 43 of the *Advertisement Law*, no organisation or individual shall, without obtaining the consent or receiving request of the parties concerned, distribute advertisements to their residence, transportation vehicle, etc.

Under Section 7.7 of the Standard, for advertising in electronic or other forms using personal data, the consent of the relevant data subject must be obtained before sending the direct marketing information. If the data subject revokes his or her consent for data processing, the data controller shall not continue sending such advertisement.

---

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

---

The CSL and the *Advertisement Law* applies 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. But 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 Chinese language, making settlement by the RMB, and delivering products to China are considered as “providing products or services to China”, in which case we understand that it is possible the relevant provisions will apply.

---

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

---

It appears that the data protection authorities are not particularly active, but there are recent cases where other authorities such as the Administration for Industry and Commerce are taking action. For example, in 2017, Shanghai Paipaidai Finance Information Service Co., Ltd. was fined RMB800,000 for its infringement of the *Advertisement Law*, the breaches include, among others, sending direct advertisements via email without obtaining prior consent of the recipients.

---

**9.5 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 strictly keep confidential a citizens' 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*.

---

**9.6 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.

---

## 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 data (the CSL stipulates that personal data refers to information which can be used alone or in combination with other information to identify a natural person, the Standard also provides that data such as the 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 onto certain third-party websites was found by the court to be not infringing 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.**

---

Article 7 of the Draft provides that the data shall not be transferred abroad in any of the following circumstances:

- (1) the personal data subject does not consent, or the outbound transmission of huge quantity of personal data jeopardises public and national interests;
- (2) the outbound transmission imposes threats on national security, economic development or public interests; or

- (3) the CAC, public security department, security authority and other relevant authorities forbid such transmission.

**11.2 Please describe the mechanisms companies 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 that such data does not satisfy any of the conditions listed under question 11.1 and a security assessment is properly carried out. For CII operators, in addition to obtaining the data subject's consent, they would need to prove that their transfer of personal data overseas arose from business needs, and would need to conduct a security assessment and submit the assessment results to competent authorities for approval.

**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 allowed, subject to the prior consent of data subject, completion of a security assessment and approval from competent industry authorities.

For other network operators, Article 8 of the Draft stipulates that, where the data satisfy the conditions listed under question 6.1, the operator should notify the relevant authorities of the information regarding the security assessments.

## 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 rule explicitly addressing this matter.

**12.2 Is anonymous reporting prohibited, or strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do companies 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 currently no unified legislation to regulate the use of CCTV apart from the *Public Security Video Image Information*

*System Administrative Regulations* (exposure draft, hereinafter the "CCTV Regulations") issued by the Ministry of Public Security which regulates the use of CCTV for public safety purposes. Its Article 20 stipulates that anyone who uses CCTV for public safety purposes shall notify the local public security department 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, the 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, 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.

## 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?**

There is no requirement to notify or consult works councils/trade unions/employee representatives.

## 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 it collects, and to establish and improve the system for user information protection. But 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.

**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) expects 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) expects 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. 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.

**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 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.

## 16 Enforcement and Sanctions

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

Investigatory Powers	Civil/Administrative Sanction	Criminal Sanction
The public security departments have investigatory power regarding criminal and administrative infringement on personal data.  The CAC, the telecommunications department and other authorities concerned have investigatory power regarding administrative infringement on personal data.	The court is responsible for the civil sanctions.  The CAC, the telecommunications department, the public security department and other authorities concerned have the power to impose administrative sanctions.	The court has the power to impose criminal sanctions.

### 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.

In 2017, the CAC and several other authorities carried out a campaign on privacy policies. They reviewed the privacy policies of 10 internet products and services including WeChat, Sina Weibo, Taobao, Alipay, Didi Chuxing, etc., seeking to send a message to other internet services and product providers. Highlights of the review included whether there was clear disclosure of the types of personal data collected and how it was collected, whether there are clear instructions on the use of personal data, (for instance, for profiling purposes), explicit notification to users regarding their rights to access, deletion and correction of their personal data, ways to achieve such rights, restrictions and so on.

### 16.4 Does the data protection authority ever exercise its powers against companies 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 against companies established in other jurisdictions.

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

### 17.1 How do companies 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 do security assessments with the relevant authority before transmitting any personal data or important data abroad. However, in terms of security assessments, the Draft Assessment Measures also provide that if there are different provisions under laws and regulations, such provisions shall apply, but in any event the consent of personal data subject is required.

And 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.

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

There is the *International Criminal Justice Assistance Act of People's Republic of China* (draft) which provides in Article 30 that the disclosure of electronic data to a foreign law enforcement agency is allowed if there are international agreements between China and such foreign country or international conventions that both countries are parties to.

## 18 Trends and Developments

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

The implementations of the CSL and other relevant legislations show that the Chinese legislators are gradually consummating the laws to protect national cyberspace sovereignty and network security. It is also a direct response to the harsh reality of personal data security currently in China. The enforcement authorities have also carried out a series of special projects.

In 2017, the Ministry of Public Security carried out a special project on cracking down internet personal data infringement crimes. As of 20 December 2017, 4,911 personal data infringement cases were solved, 15,463 suspects were caught and 164 companies involved were dismissed.

From late May to early June, 2017, the regulatory authorities launched a campaign against illegal data transactions and other data non-compliances. Brought under investigation were 15 big data companies, some of whose valuation are over billions of RMB.

In December 2017, a Consumers Council filed a civil complaint against an internet company, on the grounds that when installing two applications of the company on mobile phones, consumers are not notified about the type and purpose of the data collection. The applications require access to call monitoring, the location, messages, contacts, modify system settings, etc., without obtaining consent from the user. As a search engine and browser, the above access exceeds the reasonable scope of necessity. The court has put the case on file.

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

The illegal selling of personal data and privacy policies have been points of concern for the data protection regulators.

**Susan Ning**

King & Wood Mallesons  
40<sup>th</sup> Floor, Office Tower A  
Beijing Fortune Plaza 7  
Dongsanhuan Zhonglu  
Chaoyang District, Beijing 100020  
China

Tel: +86 10 5878 5010  
Email: [susan.ning@cn.kwm.com](mailto:susan.ning@cn.kwm.com)  
URL: [www.kwm.com](http://www.kwm.com)

Susan 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*, etc.

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.

**Han Wu**

King & Wood Mallesons  
40<sup>th</sup> Floor, Office Tower A  
Beijing Fortune Plaza 7  
Dongsanhuan Zhonglu  
Chaoyang District, Beijing 100020  
China

Tel: +86 10 5878 5749  
Email: [wuhan@cn.kwm.com](mailto:wuhan@cn.kwm.com)  
URL: [www.kwm.com](http://www.kwm.com)

Han practises in the areas of cybersecurity, data compliance and antitrust. He is good at providing cybersecurity and data compliance advice to multinational companies' branches in China from the perspective of data compliance in China. At the same time, Han can also establish 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.

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 a plan for cross-border data transfers; and assisting clients in network security investigations and cybersecurity incidents, etc.

## KING & WOOD MALLESONS 金杜律师事务所

King & Wood Mallesons is an international law firm headquartered in Asia that advises Chinese and overseas clients on a full range of domestic and cross-border transactions, providing comprehensive legal services. Around the world, the firm has over 2,000 lawyers with an extensive global network of 27 international offices spanning Singapore, Japan, the US, Australia, the UK, Germany, Spain, Italy and other key cities in Europe as well as presences in the Middle East. With a large legal talent pool equipped with local in-depth and legal practice, it provides legal services in multiple languages. King & Wood Mallesons, with its strong foundation and ever-progressive practice capacity, has been a leader in the industry. It has received more than 300 international and regional awards from internationally authoritative legal rating agencies and business and legal media, including *Acritas*, *Financial Times*, *ALB*, *Who's Who Legal*, *Chambers Asia-Pacific Awards*, *Euromoney*, *LEGALBAND*, *Legal Business*, *The Lawyer*, etc.

# Cyprus

Loizos Papacharalambous



Koushos Korfiotis Papacharalambous LLC

Anastasios Kareklas



## 1 Relevant Legislation and Competent Authorities

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

From 25 May 2018, the principal data protection legislation in the EU will be Regulation (EU) 2016/679 (the “**General Data Protection Regulation**” or “**GDPR**”). The GDPR repeals Directive 95/46/EC (the “**Data Protection Directive**”) and leads 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 N.28(III)/2001 implementing the Convention for the Protection of Individuals with regard to automatic processing of Personal Data and the Law N.30(III)/2003 implementing the Additional Protocol to the said Convention; and
- the Regulation of Electronic Communications and Postal Services Law of 2004, N.112(I)/2004 as amended to date.

### 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**”).

## 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.
- “**Special Categories of 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 interest 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 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 in Cyprus, if the data subjects lives 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?

Only notification 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 11.3.

### 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 11.3.

### 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)?

Only notifications in special circumstances: see question 11.3.

### 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)?

Only notifications in special circumstances: see question 11.3.

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

Not known yet. Please note that this answer may be subject to change by the Cypriot legislation with regards to the implementation of the GDPR which was not published at the time of writing this chapter. Please refer to the online version of the chapter for the updated answer.

### 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 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 to 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") recommends 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 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 Data Protection Officer; (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 the data subject is given the opportunity to, free of charge and easily, opt out.

**9.2 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 question 9.1.

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

This is not applicable.

**9.4 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 restrictions 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.

**9.5 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:

"Several candidates are targeting paid advertising agencies to send messages on their behalf. In these cases, candidates should themselves 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). Candidates should be able to check the list of recipients and the process of sending the messages (consent, deletion file, etc.). 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."

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

Under the Cyprus Data Protection Law, which will be replaced by the GDPR, the Commissioner may impose the following administrative sanctions in case of contravention with the obligations arising from the Law and from every other regulation concerning the protection of individuals with regard to the processing of personal data: (a) a warning with a specific time-limit for termination of the contravention; (b) a fine of up to €30,000; (c) temporary revocation of a licence; (d) permanent revocation of a licence; or (e) the destruction of a filing system or the cessation of processing and the destruction of the relevant data.

It remains to be seen how these fines will be dealt with post-May 2018. Please note that this answer was written before changes to Cypriot legislation with regards to the implementation of the GDPR were published. Please refer to the online version of the chapter for the updated answer.

## 10 Cookies

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

The Regulation of Electronic Communications and Post Law N.112(I)/2004 as amended 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 Directive 95/46/EC and, from 25 May 2018, the GDPR). For consent to be valid, it must be informed, specific, freely given and must constitute a real 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, which means that it must be essential to fulfil their request.

**10.2 The EU Commission intends to pass a new ePrivacy Regulation that will replace the respective national legislation in the EU Member States. The regulation is planned to come into force May 25, 2018 and will provide amended requirements for the usage of cookies. 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?**

No, there has been no enforcement action.

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

See question 9.6.

## 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) or the business has implemented one of the required safeguards as specified by the GDPR.



**11.2 Please describe the mechanisms companies 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.

Transfer of personal data to the US is also possible if the data importer has signed up to the EU-US Privacy Shield Framework, which was designed by the US Department of Commerce and the EU Commission to provide businesses in the EU and the US with a mechanism to comply with data protection requirement when transferring personal data from the EU to the US.

**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 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 binding corporate rules provided for in Article 47, the controller or the processor must inform the Commissioner of their intention before transferring such data.

Without prejudice to the provisions of Articles 46 and 47 of the GDPR, the Commissioner may, on serious public interest grounds, impose on the controller or the processor explicit limitations on the transfer of the specific categories of personal data.

The transmission of specific categories of personal data to a third country or to an international organisation to be carried out by a controller or processor under the derogations for specific situations provided for in Article 49 of the GDPR, requires a data protection impact assessment (“DPIA”) and prior consultation with the Commissioner.

\* Please note that this answer was written before changes to Cypriot legislation with regards to the implementation of the GDPR were published. Please refer to the online version of the chapter for the updated answer.

## 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. The WP29 recommends 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, or 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, the WP29 considers 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.

The Commissioner advises controllers to avoid anonymous reporting or to have internal procedures for handling such reporting.

## 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 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.

### 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?

The employer shall be able to justify the legality 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, in order to be justified, must prevail over the rights, interests and fundamental freedoms of employees.

### 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. For this purpose, it is good practice for the employer to adopt a written policy for determining the parameters of telephone use, computer, internet, other electronic means of communication and material/equipment of the company/organisation of employees and ways/systems with which the employer will monitor/control its use. Secret

surveillance or monitoring of employees is never permitted without the employees having been previously updated.

According to the GDPR requirements, other EU Guidance and Directives from the Commissioner, the consent as a legal basis for processing employees' personal data, which should be avoided, were possible due to the imbalance of power between the employer and the employees, which might render the consent in question as not freely given or unambiguous.

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

According to the Commissioner's guidelines on the subject, 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 Powers *	Civil/Administrative Sanction *	Criminal Sanction *
* Please note that this answer may be subject to change by the Cypriot legislation with regards to the implementation of the GDPR which was not published at the time of writing this chapter. <a href="#">Please refer to the online version of the chapter for the updated answer.</a>	* Please note that this answer may be subject to change by the Cypriot legislation with regards to the implementation of the GDPR which was not published at the time of writing this chapter. <a href="#">Please refer to the online version of the chapter for the updated answer.</a>	* Please note that this answer may be subject to change by the Cypriot legislation with regards to the implementation of the GDPR which was not published at the time of writing this chapter. <a href="#">Please refer to the online version of the chapter for the updated answer.</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.	N/A
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).	N/A
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.	N/A

<b>Investigatory Powers *</b>	<b>Civil/Administrative Sanction *</b>	<b>Criminal Sanction *</b>
* Please note that this answer may be subject to change by the Cypriot legislation with regards to the implementation of the GDPR which was not published at the time of writing this chapter. <a href="#">Please refer to the online version of the chapter for the updated answer.</a>	* Please note that this answer may be subject to change by the Cypriot legislation with regards to the implementation of the GDPR which was not published at the time of writing this chapter. <a href="#">Please refer to the online version of the chapter for the updated answer.</a>	* Please note that this answer may be subject to change by the Cypriot legislation with regards to the implementation of the GDPR which was not published at the time of writing this chapter. <a href="#">Please refer to the online version of the chapter for the updated answer.</a>
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 proceeding financial year.	N/A
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 proceeding financial year, whichever is higher.	N/A

#### **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.

Please note that this answer may be subject to change by the Cypriot legislation with regards to the implementation of the GDPR which was not published at the time of writing this chapter. [Please refer to the online version of the chapter for the updated answer.](#)

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

This information is not available yet.

Please note that this answer was written before changes to Cypriot legislation with regards to the implementation of the GDPR were published. [Please refer to the online version of the chapter for the updated answer.](#)

#### **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 note that this answer may be subject to change by the Cypriot legislation with regards to the implementation of the GDPR which was not published at the time of writing this chapter. [Please refer to the online version of the chapter for the updated answer.](#)

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

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

Data exporters must inform the Commissioner of any third-country legislation that the data importer is subject to, providing for the statutory disclosure of the transferred data to public authorities of that country.

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

The Commissioner advises data exporters to scrutinise such legislations against the WP29 Working Document titled "Essential Guarantees".

### **18 Trends and Developments**

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

There is no relevant case law issued in the past 12 months.

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

The office of the Commissioner has been focusing on the prevention of false practices in breach of the Data Protection Laws by both the public and private sector, and in so doing, has issued guidance about a) the DPIAs, b) Records of Processing Activities (Article 30 of the GDPR), c) Certification Bodies, and d) Retention Policies by Authorised Credit Institutions. The Commissioner has also advised for vigilance with cybersecurity threats and also with how third parties may unlawfully process consumers' and users' data.



**Loizos Papacharalambous**

Koushos Korfiotis Papacharalambous LLC  
20 Costis Palamas str.  
Aspelia Court  
1096 Nicosia  
Cyprus

Tel: +357 22 664 555  
Email: loizosp@kkplaw.com  
URL: www.kkplaw.com

Loizos 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 College of the University of London. In 2011, Loizos was admitted as a Member of The Chartered Institute of Arbitrators. Loizos is currently attending courses to obtain a 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.

**Anastasios Kareklas**

Koushos Korfiotis Papacharalambous LLC  
20 Costis Palamas str.  
Aspelia Court  
1096 Nicosia  
Cyprus

Tel: +357 22 664 555  
Email: akareklas@kkplaw.com  
URL: www.kkplaw.com

Anastasios is a lawyer at Koushos Korfiotis Papacharalambous LLC, with wide-ranging knowledge and experience on IT legal matters both on academic and business levels, with a particular focus on e-Commerce Law and Data Protection 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 acts as Data Protection Advisor 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 for clients.

**KOUSHOS KORFIOTIS PAPACHARALAMBOUS LLC**

ADVOCATES & LEGAL CONSULTANTS

Koushos Korfiotis Papacharalambous 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, 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*.

# France

Benjamin Potier



Clyde & Co

Jean-Michel Reversac



## 1 Relevant Legislation and Competent Authorities

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

From 25 May 2018, the principal data protection legislation in the EU will be Regulation (EU) 2016/679 (the “**General Data Protection Regulation**” or “**GDPR**”). The GDPR repeals Directive 95/46/EC (the “**Data Protection Directive**”) and leads to increased (though not total) harmonisation of data protection law across the EU Member States.

The French parliament is discussing the vote of a new law to include and complete the GDPR Regulation into the French system (bearing in mind that GDPR Regulation is applicable *per se*); this “new” French law shall be passed by 25 May 2018 and completed by a decree redrafting the law n° 78-17 dated 6 January 1978.

GDPR Regulation shall, indeed, be integrated within the existing French law n° 78-17 dated 6 January 1978 relating to computer programs, files and freedoms (*loi relative à l’informatique, aux fichiers et aux libertés*). This French law is the “heart” of the French regulation relating to personal data.

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

The French post and electronic communications code includes the article L. 34-5, which prevents the sending of fax and emails to consumers without their prior consent, in accordance with the requirements of Directive 2002/58/EC (as amended by Directive 2009/136/EC) (the “**ePrivacy Directive**”). In January 2017, the European Commission published a proposal for an ePrivacy Regulation that would harmonise the applicable rules across the EU.

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

The French authority responsible for data protection – the National Commission for Computing and Freedom, i.e. *Commission Nationale de l’Informatique et des Libertés* – “**CNIL**” – may issue guidelines with regard to the processing of genetic data, biometric data or data concerning health, in accordance with article 9, 4 of GDPR.

Dealing with personal data in relation to criminal law is subject to a dedicated Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977.

The purpose of this EU Directive will be transposed into French regulation by a law in course of discussion before the French parliament.

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

The CNIL is the French body 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).

French additional regulation on personal data applies to individuals residing in France, except for processing carried out for journalistic purposes or the purpose of academic, artistic or literary expression, which shall be subject to the home state law of the controller.

### 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 interest 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 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 in France, i.e. the 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?

Before the GDPR regulation, companies acting in France had to notify the French control authority that they were dealing with personal data. With the new GDPR Regulation, this obligation is withdrawn and the obligation of the controller is to hold a record of processing activities in accordance with articles 30 and 31 of the GDPR Regulation (Accountability principle – see question 4.1).

The obligation to hold records shall not apply to an enterprise employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects and the processing is not occasional.

With regards to the actual draft of French law for the transposition of the GDPR Regulation, prior approval would still exist for data collected by the French state concerning genetic and biometric data. Decree(s) will be adopted by the relevant French State body and set the process for such prior approval.

With regards to the actual draft of French law for the transposition of the GDPR regulation, collecting data concerning health will not need prior approval by the CNIL but will have to be done in accordance with a framework approved by the CNIL and *l’Institut national des données de santé* – article 13.

For the next 10 years, existing list of personal data registered with the CNIL will be accessible to the public.

### 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)?

No EU standard response. 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)?

No EU standard response. 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)?

No EU standard response. 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)?

No EU standard response. See question 6.1 above.



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

No EU standard response. See question 6.1 above.

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

No EU standard response. See question 6.1 above.

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

No EU standard response. See question 6.1 above.

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

No EU standard response. See question 6.1 above.

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

No EU standard response. See question 6.1 above.

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

No EU standard response. See question 6.1 above.

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

No EU standard response. 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.

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 – see questions 15.4 and 16.1.

## 7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect to 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 for 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.

The French CNIL plans to appoint a certification body which will be empowered to deliver Data Protection Officer certification.

A French association of Data Protection Officers (*L'Association française des correspondants à la protection des données à caractère personnel* – [www.afcdp.net](http://www.afcdp.net)) has drafted a charter of ethics for the Data Protection Officer; the Data Protection Officer may decide to adhere to this charter.

## 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”) recommends 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 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 Data Protection Officer; (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?)

A prior authorisation shall be expressly obtained before sending direct marketing to consumers (see article L. 34-5 of the French post and electronic communications code regarding fax and emails). Any consumer receiving telephone or SMS spam may transfer them to “33 700” and block the telephone or SMS spam.

### 9.2 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 consumer may register in a list of opposition to out-bound calls,

called *Bloctel* ([www.bloctel.gouv.fr](http://www.bloctel.gouv.fr)). The registration on that list is 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 was a previous 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:

- The company shall nevertheless inform the consumer that he/she may declare its opposition to future marketing calls.
- The company is no longer entitled to call the consumer after the end of the concerned service (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.

### 9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

The GDPR regulation protects the persons residing within the EU. EU citizens must agree to receive marketing emails. In this regard, marketing sent from other jurisdictions should comply with EU regulations concerning the sending of marketing emails from other jurisdictions.

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

The consumer may file a claim online with *Bloctel* against companies calling him/her in breach of his/her registration on that list ([www.bloctel.gouv.fr](http://www.bloctel.gouv.fr)) or with the CNIL relating to telephone or SMS spam.

### 9.5 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 lists from third parties is lawful. However, the purchaser of the list shall ensure that the seller of the lists has obtained the express agreement of consumers that their data be transferred to third parties and must check that the phone number is not registered on the Bloctel list.

### 9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

The maximum criminal penalties are five years’ imprisonment and a fine of €300,000 (for individuals) or €1.5 million (if the company is held liable). In addition, a maximum administrative fine of €20 million may be imposed by the CNIL for failure to comply with GDPR requirements (see question 16.1 below).

## 10 Cookies

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

Article 32, II of the French law n° 78-17 dated 6 January 1978

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 Directive 95/46/EC and, from 25 May 2018, the GDPR). For consent to be valid, it must be informed, specific, freely given and must constitute a real 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, which means that it must be essential to fulfil their request.

**10.2 The EU Commission intends to pass a new ePrivacy Regulation that will replace the respective national legislation in the EU Member States. The regulation is planned to come into force May 25, 2018 and will provide amended requirements for the usage of cookies. Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?**

See question 10.1 above.

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

The French control authority CNIL has issued rules concerning cookies, which are close to the ones issued by the WP29: the prior consent of the person visiting a website shall be obtained (subject to exceptions: see question 10.1 above); this prior consent is valid for 13 months (see [www.cnil.fr/fr/cookies](http://www.cnil.fr/fr/cookies)).

In the course of 2016, the CNIL launched an inquiry over 13 websites concerning their use of cookies.

On 23 March 2017, the CNIL sentenced a major web company to a €150,000 penalty for lack of information of the users of its website concerning cookies used by this website and the impossibility to refuse cookies.

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

The CNIL may impose a maximum administrative fine of €3 million or €20 million, depending on the future interpretation of the scope of GDPR Regulation (see question 16.1 below).

## 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) or the business has implemented one of the required safeguards as specified by the GDPR.

**11.2 Please describe the mechanisms companies 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.

Transfer of personal data to the US is also possible if the data importer has signed up to the EU-US Privacy Shield Framework, which was designed by the US Department of Commerce and the EU Commission to provide businesses in the EU and the US with a mechanism to comply with data protection requirements when transferring personal data from the EU to the US.

**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.

## 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, 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. The WP29 recommends 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.

Under French law, some provisions protect whistle-blowers against any discrimination regarding their salary, professional evolution with regards to conflict of interest concerning a state representative, corruption (article L. 1132-3-3 of the French labour code), serious risk to the health, the environment or the safety of sanitary or cosmetic products, moral or sexual harassment (articles L. 1152-1 and further and article L. 1153-1 and further of the French labour code), discrimination (article L. 1132-3 of the French labour code), serious danger for his/her life or health, defective protection systems (article L. 4131-1 of the French labour code). No specific provision is dedicated to the protection of personal data.

#### **12.2 Is anonymous reporting prohibited, or 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, the WP29 considers 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.

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

A CCTV system shall not be used directly to watch employees, unless their work is critical (dealing with money, stock of high-value goods). A CCTV system shall not film restrooms, rooms dedicated to unions, and toilets. Films shall be erased after one month. Public notices shall be put on walls.

## **14 Employee Monitoring**

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

Geolocation of vehicles driven by employees is possible, but with some prohibitions; this system is not allowed to collect information when the driver is outside his/her working time, to check the moving of union representatives. Drivers shall be informed that a geolocation system is on the car. The driver may be able to deactivate the system outside his/her working time. Collected information may be kept for two months, one year or five years, depending on the purpose of the installation of this system.

Registration of phone calls is allowed for training or evaluation of employees. Employees may deactivate the registration system or be provided with phones not linked to a registration system. Conversations of union representatives cannot be registered. In most cases, registration of phone calls shall be erased after six months.



The control of access to offices and the check of working time is possible by the use of access cards to the offices. Information may be kept for three months or five years.

The employer may control the use of the computer, access to internet and emails exchanged by the employees, unless the email was quoted “as personal/private”.

---

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

---

Employees shall be informed that their activity is subject to employee monitoring tools. They cannot oppose it if the installation is necessary and corresponds to the legal limit which authorises the installation of such tools. But employees shall not be “controlled” outside their working time.

Only authorised persons may have access to information collected by way of the employee monitoring tools.

---

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

---

Unions shall be consulted before the installation of employee monitoring tools (article L. 2323-47 and L. 2312-38 of the French labour code). Otherwise, the employer is subject to criminal sanctions.

## **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?**

---

As first sanctions, the French control authority CNIL may pronounce the following measures: a reminder; and/or an injunction to comply with the regulation with an eventual penalty up to €100,000 per day. In major cases, the CNIL may also pronounce a penalty up to €10 million or 4% of the worldwide turnover. The maximum penalty is the higher of €20 million or 4% of worldwide turnover in the event of breaches sentenced by points 5 and 6 of article 83 of the GDPR Regulation.

## 16 Enforcement and Sanctions

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

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
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.	The CNIL may refer the case to the French public prosecutor, or a data subject may raise a criminal complaint and a French judge may impose a criminal sanction which may lead to up to five years' imprisonment and a fine of up to €300,000 (for individuals) to €1.5 million (if a company is held liable).  In addition, if a criminal procedure is engaged, the criminal judge can decide to take into account the amount of the administrative fine to determine the amount of the criminal fine (article 6, 7° of the draft of the French law of 13 February 2018).
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).	
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.	
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 proceeding financial year.	
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 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. The relevant French regulation provides that the French control authority CNIL may issue such temporary or final ban.

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

Considering that GDPR is a very new regulation still not in force, no case exists in this matter. It is nevertheless interesting to note that the French authority CNIL may intervene before courts that will deal with GDPR issues and express observations.

Agents of the CNIL may claim for communication of any documents and make copies, and can have access to computer programs, to the extent that the concerned information is not privileged (exchanges between a client and lawyers, health data, sources of journalists).

Agents of the CNIL may perform any online transaction necessary for their mission under a borrowed identity.

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

The French control authority CNIL may collaborate with other EU control authorities in accordance with articles 60 to 67 of the GDPR Regulation.

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

### 17.1 How do companies 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 to the extent that such requests comply with some 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 shall be limited to a fixed period; the claimant shall disclose security measures taken to manage 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/EU.

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

The WP29 has issued a working document on 2009 (WP158), which has inspired the work done by the French CNIL on 23 July 2009 relating to guidelines concerning discovery requested by US agencies (decision n°2009-474).

## 18 Trends and Developments

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

A recent decision of the French control authority CNIL of 8 January 2018 sentenced a major distributor with a €100,000 penalty: the distributor as controller delegated the management of personal data to a processor; further to a claim notified to the CNIL, it noticed that non-authorised persons may consult the personal data; and the French control authority CNIL ruled that the distributor was liable for the mismanagement by its sub-contractor acting as processor.

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

A recent French law n° 2016-1547 of 18 November 2016 authorises group action engaged by consumers facing the same issue relating to the mismanagement of their personal data by the same controller or processor. The developments of such action in the future could be an important issue in the coming years.

An association may be empowered by any concerned person to exercise its rights on his or her behalf under articles 77 to 79 and 82 of the GDPR regulation against the French control authority CNIL or the controller or the processor, if the breach of the regulations relates to a criminal matter.



### Benjamin Potier

Clyde & Co  
134 Boulevard Haussmann  
75008 Paris  
France

Tel: +33 1 4443 8996  
Email: [Benjamin.Potier@clydeco.fr](mailto:Benjamin.Potier@clydeco.fr)  
URL: [www.clydeco.com](http://www.clydeco.com)

Benjamin practises litigation before civil, commercial, administrative and criminal courts. He acts for major companies both domestic and international. He is interested in various fields such as transportation, insurance, banking and new areas such as data protection.

His is recognised by *Who's Who Legal* and *The Legal 500*.



### Jean-Michel Reversac

Clyde & Co  
134 Boulevard Haussmann  
75008 Paris  
France

Tel: +33 1 4443 8975  
Email: [Jean-Michel.Reversac@clydeco.fr](mailto:Jean-Michel.Reversac@clydeco.fr)  
URL: [www.clydeco.com](http://www.clydeco.com)

Jean-Michel is a Legal Director focusing on business, corporate, insurance and reinsurance law and drafting agreements requiring special care on the protection of personal data.

Having practised for over 20 years, Jean-Michel handles mergers and acquisitions, international agreements and commercial leases. His wide commercial practice encompasses both advice and litigation. Jean-Michel regularly advises on the establishment, structuring of new entities and on group restructurings, and has substantial experience in advising foreign companies on investing in the French market (from counselling to litigation) on business law and corporate law matters.

His insurance and reinsurance practice entails commercial drafting and reviewing of general terms of insurance policies. He represents all parties in the distribution and management of insurance policies. Much of his work relates to cross-border business and regulatory aspects of the insurance sector. In addition, he advises insurers on European and French operations.

## CLYDE & CO

We provide businesses with full-service data protection and privacy advice across all industry sectors, enabling clients to focus their resources on other business needs.

Data privacy and protection is absolutely fundamental to all types of organisation due to the increasing threat of malicious hackers with the ability to leverage and monetise information.

Multi-national organisations face a web of complex and conflicting laws and regulations surrounding the collection, use, retention and disclosure of information. This requires careful attention to data privacy at every stage of the business cycle to avoid the negative publicity surrounding data breaches.

Our team brings together a wealth of experience across a range of sectors and industries to keep you on the cutting edge of developments in the industry. Our strong working relationships with the regulators and industry bodies enable us to resolve issues and provide practical commercial advice.

We advise a wide range of businesses including retailers, insurers, hospitals, information service providers, technology start-ups, financial institutions, educational institutions and governments across the world on the full range of data issues.

# Germany

GÖRG Partnerschaft von Rechtsanwälten mbB

Dr. Katharina Landes



## 1 Relevant Legislation and Competent Authorities

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

From May 25, 2018, the principal data protection legislation in the EU will be Regulation (EU) 2016/679 (the “**General Data Protection Regulation**” or “**GDPR**”). The GDPR repeals Directive 95/46/EC (the “**Data Protection Directive**”) and leads 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 German Federal Data Protection Act (*Bundesdatenschutzgesetz*) (“**FDPA**”) will come into effect in a new version on May 25, 2018. The FDPA provides specific provisions for the federal public sector but also provisions for the private sector which are based on certain “opening clauses” contained in the GDPR. The 16 German federal states also have state-level data protection laws which will also be adapted to the GDPR. These laws only apply to the public sector in the relevant state.

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

The Telecommunications Act (*Telekommunikationsgesetz*) contains sector-specific data protection provisions that apply to telecommunications services providers such as internet access providers. The Telemedia Act (*Telemediengesetz*) also contains sector-specific data protection provisions that apply to telemedia service providers such as website providers. However, the Telemedia Act will be replaced by the rules of the ePrivacy Regulation. The Social Security Codes (*Sozialgesetzbücher*) contain specific data protection provisions concerning the processing of social data by social security institutions. Specific rules for direct marketing (telephone, fax, email, SMS, etc.) are set out in the Unfair Competition Act (*Gesetz gegen den unlauteren Wettbewerb*).

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

There are 16 state data protection authorities which oversee and enforce private sector data protection compliance of entities

established in their state. In addition, the federal data protection commissioner (*Bundesdatenschutzbeauftragter*) oversees and enforces data protection compliance within the federal public sector (e.g., federal ministries), as well as certain parts of the postal services and telecommunications services providers’ activities. The federal data protection commissioner also represents the 16 state authorities in the European Board.

## 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.
- *Other key definitions – please specify (e.g., “Pseudonymous Data”, “Direct Personal Data”, “Indirect Personal Data”).*  
There are no other specific key definitions.



### 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 interest 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 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, in particular, the competent data protection authority in Germany, (according to German legal literature, article 77 of the GDPR allows data subjects to file a complaint with any data protection authority in the European Union and, in particular, with the data protection authorities in Germany) if the data subjects live or work 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, 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 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 which is subject to a data protection impact assessment; (iv) commercial processing of personal data for the purpose of (anonymised) transfer or for the purpose of market or opinion research; or (v) there are at least 10 persons permanently employed for the automatic 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 to 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") recommends 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 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 Data Protection Officer; (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?)

The Unfair Competition Act generally requires the recipient's express prior consent if marketing messages are sent to him/her by phone, SMS, fax or email. However, there are exceptions for email marketing. Section 7 (3) of the Unfair Competition Act allows marketing emails to be sent without the recipient's consent (therefore opt-out is sufficient) where the following conditions are met cumulatively:

- the company obtained the recipient's email address from the recipient in connection with the sale of a good or a service;
- the company uses the email address to advertise directly for similar and own goods or services;
- the recipient has not objected to such use; and
- at the time the email address is collected as well as each time it is used, the recipient is informed clearly and unambiguously that he/she can object to such use at any time without incurring transmission costs which exceed the basic transmission tariffs.

### 9.2 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 and fax an express consent is required by the Unfair Competition Act as well. For marketing by post, there are no consent or opt-out requirements.

### 9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

Yes. The Unfair Competition Act applies to marketing activities which have impact on the German market so that marketing sent from other jurisdictions to German market participants is subject to the above restrictions as well.

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

Yes. Enforcement action, as well as litigation concerning breaches of marketing restrictions, is frequent in Germany.

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

There are no specific German provisions on this topic (except for

those set out in questions 9.1 and 9.2 above), so the general rules of the GDPR apply (legitimate interests pursued by the controllers, sufficient information of the data subject, in particular about the right to object, etc.).

### 9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

Breaches of the Unfair Competition Act's marketing restrictions regarding phone marketing can result in fines of up to €300,000 (section 20 (2) of the Unfair Competition Act).

## 10 Cookies

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

There is no legislation specifically dealing with the use of cookies. However, section 15 of the Telemedia Act sets out rules for the processing of personal data generated during the use of a telemedia service. According to section 15 (1), the service provider is only allowed to collect and use personal user data without consent of the user as far as this is necessary to provide the telemedia service. Furthermore, section 15 (3) of the Telemedia Act sets out that the service provider may create user profiles under a pseudonym for marketing purposes provided that the user has not objected.

The German government's position is that only those cookies that are strictly necessary for the user to receive telemedia services (e.g., to view a website) can be used without the user's prior opt-in consent. The German government's position is outlined in a communication to the European Commission (COCOM11-20) dated October 4, 2011. The German data protection authorities, though, issued a resolution dated February 5, 2015 in which they request the German government to implement the requirement of the ePrivacy Directive (article 5 (3) for opt-in consent for cookies). However, there hasn't been an amendment of the Telemedia Act since then.

There are currently conflicting opinions in legal literature as to whether the data protection rules of the Telemedia Act are applicable under the GDPR. Some are of the opinion that these rules must be applied as long as the new ePrivacy Regulation has not come into force, while others say that these rules are replaced by the rules of the GDPR.

### 10.2 The EU Commission intends to pass a new ePrivacy Regulation that will replace the respective national legislation in the EU Member States. The regulation is planned to come into force May 25, 2018 and will provide amended requirements for the usage of cookies. Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

Please refer to the answer above.

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

Yes. The Bavarian Data Protection Authority ("DPA") has analysed various web analytics tools in detail and made recommendations on how such tools can be used in a compliant manner. Cookies and opt-out methods played a central role in these analyses.



The Federation of German Consumer Organisations (*Bundesverband der Verbraucherzentralen*) initiated court proceedings against a company which used a pre-checked box to obtain the consent to web tracking measures for marketing purposes from entrants of a prize competition. In the course of the proceedings, the German Federal Court (decision of October 5, 2017, I ZR 7/16) submitted to the European Court of Justice the question whether a valid consent to the use of cookies in the meaning of article 5 (3) and article 2 lit. f of the Directive 2002/58/EG in conjunction with article 2 lit. h of the Directive 95/46/EG can be lawfully obtained by using a pre-checked box.

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

Breaches of the relevant provisions of the FDPA could result in fines of up to €300,000. Breaches of the relevant provisions of the Telemedia Act could result in fines of up to €50,000.

### 11 Restrictions on International Data Transfers

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

Data transfers to 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) or the business has implemented one of the required safeguards as specified by the GDPR.

#### 11.2 Please describe the mechanisms companies 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.

Transfer of personal data to the US is also possible if the data importer has signed up to the EU-US Privacy Shield Framework, which was designed by the US Department of Commerce and the EU Commission to provide businesses in the EU and the US with a mechanism to comply with data protection requirement when transferring personal data from the EU to the US.

#### 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.

### 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. The WP29 recommends 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, or 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, the WP29 considers 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.

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

Yes. Video surveillance of publicly accessible places is only legitimate where it is necessary: (i) to fulfil duties of public authorities; (ii) to exercise the householder's rights; and (iii) for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests of the data subject (section 4 FDPA).

## 14 Employee Monitoring

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

Employee monitoring is only permitted in very limited circumstances since the relevant legal basis (section 26 FDPA) is a specific provision for employee data processing. For example, data controllers may process personal data of employees if it is necessary

to discover crimes or severe breaches of the employee's contractual obligations, but only if: (a) there are documented factual indications which support the suspicion that the employee has committed a crime or has severely breached the employment contract in the course of the employment relationship; (b) the processing of personal data is necessary to discover the crime/the severe breach; and (c) the protected privacy interests of the employee do not take precedence.

Permanent monitoring of employees via CCTV is usually not permitted and companies have been fined for doing so. Sporadic monitoring for quality and training purposes (e.g., listening in on customer calls) may be lawful provided that it is not excessive and the relevant legal requirements (e.g., notice) are met.

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

Under the former FDPA, the data protection authorities considered that, in an employment context, consent is not a valid legal basis for the processing of personal data since employees were rarely free to give or withhold consent demanded by the employer. Section 26 FDPA now sets out that the consent of an employee generally can be a legal basis for the processing but it must be given voluntarily and in writing. Section 26 FDPA presumes that the consent has been given voluntarily, for example, when the processing leads to a benefit for the employee, or when controller and employee pursue the same interests with regard to the processing. However, as monitoring measures do not fall under these examples, consent still would not be considered as freely given. Therefore, the employer needs to ensure that any monitoring of employees that involves the processing of personal data is covered by section 26 FDPA. In addition to the legal basis, the employer must provide advance and sufficiently detailed notice of any employee monitoring. Where the employer has a works council, a works council agreement will usually be required to legitimise the employee monitoring. Employees must then be made aware of these works council agreements, which is usually done via email or another type of prominent notice.

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

Section 87 Nos. 1 and 6 of the Works Constitution Act (*Betriebsverfassungsgesetz*) requires that the works council must be informed about, and agree to, all measures that concern how the employees' behaviour is regulated (No. 1) and whenever technical means to monitor the employees' behaviour and performance are to be introduced (No. 6). This process usually takes several months.

## 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 Power	Civil/Administrative Sanction	Criminal Sanction
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.	N/A
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).	N/A
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.	N/A
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.	According to section 42 FDPA, certain intentional violations of data protection rules constitute a crime. For example, the professional, unlawful transfer of not publicly available personal data of a big number of data subjects can be punished by a fine or by imprisonment of up to three years.

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
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 proceeding financial year, whichever is higher.	N/A

#### 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.

German data protection authorities exercise their enforcement powers reasonably frequently. Most common are audits (whether by way of questionnaire or on-site inspection) as well as specific compliance orders. Where serious breaches occurred or orders are not complied with, German data protection authorities impose fines. Notable cases include a €1.1 million fine imposed on Deutsche Bahn for multiple breaches of the FDPA, as well as a €1.5 million fine imposed on the Lidl group for using private detectives and secret cameras in their German shops.

Recent cases concerned a fine of €15,000 imposed on a credit agency by the Hamburg DPA. The agency had created scoring values concerning the creditworthiness of a person only based on the area where the person resided.

The Bavarian DPA fined a company which appointed an employee as the data protection officer who had a conflict of interests since the employee was also the IT manager of the company.

For further cases, see section 18 below.

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

In 2017, the Hamburg DPA imposed a ban on Facebook Ireland Ltd. concerning the use of personal data of millions of WhatsApp users by Facebook without a valid consent of the users. After Facebook had filed an urgent motion against the ban, the Higher Administrative Court of Hamburg (decision of February 26, 2018, 5 Bs 93/17) confirmed the ban as legitimate. However, due to the character of summary proceedings, the Court expressly left open the questions whether German data protection law was applicable and, if so, whether the Hamburg DPA was allowed to proceed against Facebook having its place of business in Ireland.

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

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

In our experience, German companies tend to refer foreign public authorities to the relevant mutual legal assistance treaties so that disclosures of personal data are done in a manner compliant with German data protection law. Where e-discovery requests are concerned, German companies tend to pseudonymise or anonymise the relevant materials first, before they are transferred.

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

Where direct disclosure requests/orders by foreign public authorities are concerned, the German data protection authorities have stated that the relevant German authorities should be involved immediately so that the disclosure can be done in accordance with relevant mutual legal assistance treaties (see the Berlin Data Protection Authority's statement dated November 14, 2008, as well as the German Federal Ministry of Justice's letter to the Berlin Data Protection Authority dated January 31, 2007). As regards foreign e-discovery requests/orders, the German data protection authorities' position is that in light of the WP29's paper on this topic (WP158) as well as the Hague Convention, there must not be a transfer of personal data abroad before proceedings have been issued (i.e., pre-trial). Once the proceedings are underway, though, personal data can be transferred in pseudonymised form and data such as individual names may be de-pseudonymised as required on a case-by-case basis (see section 11.3 of the Berlin Data Protection Authority's 2009 report).

## 18 Trends and Developments

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

The monitoring of employees is often the subject of court decisions. For example, the groundless use of key-logger technology to monitor employees is considered as a breach of data protection rules (Federal Labour Court, decision of July 27, 2017, 2 AZR 681/16). The engagement of a private investigator to spy on an employee, though, can be legitimate provided that there are documented factual indications which support the suspicion that the employee has severely breached the employment contract (e.g. breach of a competition clause, Federal Labour Court, decision of June 29, 2017, 2 AZR 597/16).

Furthermore, data protection authorities and courts have been repeatedly concerned with the use of dash cams in private cars which they consider an unlawful processing of personal data in case that the dash cam is permanently active.

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

The alleged sale of customer data (e.g., information regarding buying power, age, gender, education, housing situation, car



ownership, etc.) to political parties by Deutsche Post Direkt GmbH (a subsidiary of the biggest German postal operator) is currently being examined by the North Rhine-Westphalian DPA (April 2018).

In June/July 2017, the Bavarian DPA reviewed 40 companies with regard to their use of the marketing tool “Facebook Custom Audience” which enables companies to target their advertising on Facebook. In case that the company transmits the customer’s email address to Facebook in order to use the tool, the DPA claims that the informed consent of the customer must be obtained.

In April 2017, the Consumer Association of North Rhine-Westphalia presented the results of a study on the compliance of fitness apps and wearables with regard to data protection. The study shows that most of the 24 apps and 12 devices were not compliant. In particular, the users’ health data was unlawfully transmitted to the app/device provider and the users were inadequately informed about what happened to their data. The Consumer Association sent warning letters to some of the app/device providers (Garmin, Fitbit, Technaxx, Striiv, Jawbone and Apple). Since Apple did not undersign the requested cease and desist declaration, the Consumer Association has brought the case to trial.



#### Dr. Katharina Landes

GÖRG Partnerschaft von Rechtsanwälten mbB  
Kennedyplatz 2  
50679 Köln  
Germany

*Tel:* +49 221 3366 0284

*Email:* [klandes@goerg.de](mailto:klandes@goerg.de)

*URL:* [www.goerg.de](http://www.goerg.de)

Dr. Katharina Landes has been working as an attorney at GÖRG for more than 11 years. Her core specialisations are data protection, information technology, intellectual property and commercial. She is the data protection officer of the firm and has in-depth experience in advising national and international clients of all industry sectors (e.g., healthcare, energy, logistics, consumer goods, media, retail, etc.) on a broad range of data protection matters. Recently, she mostly advised clients on the implementation of GDPR-compliant structures and operating procedures. She also regularly advises clients on software and outsourcing projects (including litigation), on e-commerce and other online services as well as on IP matters, such as trademark and copyright infringement.



GÖRG is one of Germany’s leading business law firms. Nationwide, the firm ranks among the top 20 law firms. As an independent law firm with 270 lawyers at six offices in Berlin, Cologne, Essen, Frankfurt am Main, Hamburg and Munich, GÖRG advises on the core areas of business law. GÖRG has a leading reputation in insolvency law and restructuring projects and is top-ranked in all core areas of business law. Our clients include renowned companies both in Germany and abroad. We have a wealth of experience, particularly in advising banks and financial service providers, real estate and energy companies as well as clients in the media and service sector.

# Hong Kong

Joshua Cole



Hoi Tak Leung



## Ashurst Hong Kong

### 1 Relevant Legislation and Competent Authorities

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

Hong Kong's principal data protection legislation is the *Personal Data (Privacy) Ordinance (Cap. 486)* (the "PDPO").

The PDPO came into force in 1996, and was one of Asia's earliest comprehensive data privacy legislation. The PDPO is based on the Organisation for Economic Co-operation and Development's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, which in turn was a foundation for Europe's *Data Protection Directive EC95/46*. The PDPO was last amended in 2012, primarily in relation to direct marketing-related obligations.

All clause references in this chapter are to the PDPO, unless otherwise expressly specified.

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

Except for the PDPO, there is no general data protection legislation.

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

While there is no sector-specific data protection legislation:

- the Office of the Privacy Commissioner for Personal Data ("PCPD") has issued various Guidance and codes of practice on how the PDPO applies in various contexts. While these documents are not the law *per se*, they represent the Privacy Commissioner for Personal Data's (the "Commissioner") views on PDPO compliance, and failure to comply with them will weigh unfavourably against the relevant data user in any case before the Commissioner;
- various regulators and industry associations have issued guidelines and codes of practice that may affect how data protection is addressed in those industries. For example, the Hong Kong Monetary Authority (the "HKMA") has issued a *Circular on Customer Data Protection* and a *Supervisory Policy Manual on Risk Management of E-banking*, and the HKMA, Securities and Futures Commission (the "SFC") and the Insurance Authority have all published guidelines on outsourcing – these documents contain provisions that are relevant to data protection; and
- there are various legislation that impact data protection-related areas. For example, a number of statutes allow

government bodies to access or compel disclosure of personal data:

- Section 44 allows the Commissioner to require the furnishing of information or documentation relevant to an investigation.
- The *Interception of Communications and Surveillance Ordinance (Cap. 589)* enables law enforcement authorities to intercept communications and carry out covert surveillance subject to certain requirements.
- Section 52 of the *Inland Revenue Ordinance (Cap. 112)* enables the Inland Revenue Department to require an employer to furnish information on an employee.
- Various ordinances give public authorities/regulators the power to compel disclosure of information in relation to financial crimes – e.g. the *Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance (Cap. 615)*.

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

The PCPD was established by the PDPO, and is an independent statutory body that enforces the PDPO. This Office is headed by the Commissioner. The current Commissioner is Mr. Stephen Wong Kai-Yi, appointed on 4 August 2015. As of June 2017, the PCPD had a total of 76 staff members across six divisions.

### 2 Definitions

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

Unless otherwise specified, the following definitions are from the PDPO.

Term	Definition under the PDPO (if applicable)
"Personal Data"	Means any data: (a) relating directly or indirectly to a living individual; (b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and (c) in a form in which access to or processing of the data is practicable.

Term	Definition under the PDPO (if applicable)
“Processing”	In relation to personal data, includes amending, augmenting, deleting or rearranging the data, whether by automated means or otherwise.
“Controller”	“Data User” is the equivalent term for data controller under the PDPO. “Data User” in relation to personal data means a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data.
“Processor”	“Data Processor” means a person who: (a) processes personal data on behalf of another person; and (b) does not process the data for any of the person’s own purposes. Note that PDPO obligations are on the data user, including in relation to ensuring that any engaged data processors also comply with relevant PDPO provisions.
“Data Subject”	In relation to personal data, means the individual who is the subject of the data.
“Sensitive Personal Data”	This is not applicable in our jurisdiction. “Sensitive Personal Data” is not defined under the PDPO.
“Data Breach”	This is not applicable in our jurisdiction. “Data Breach” is not defined under the PDPO.

Other key definitions under the PDPO	
“Data”	Means any representation of information (including an expression of opinion) in any document, and includes a personal identifier.
“Document”	Includes, in addition to a document in writing: (a) a disc, tape or other device in which data other than visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced from the disc, tape or other device; and (b) a film, tape or other device in which visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced from the film, tape or other device.
“Direct marketing”	Means: (a) the offering, or advertising of the availability, of goods, facilities or services; or (b) the solicitation of donations or contributions for charitable, cultural, philanthropic, recreational, political or other purposes, through direct marketing means.
“Direct marketing means”	Means: (a) sending information or goods, addressed to specific persons by name, by mail, fax, electronic mail or other means of communication; or (b) making telephone calls to specific persons.

Other key definitions under the PDPO	
“Personal identifier”	Means an identifier: (a) that is assigned to an individual by a data user for the purpose of the operations of the user; and (b) that uniquely identifies that individual in relation to the data user, but does not include an individual’s name used to identify that 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 PDPO does not confer extra-territorial application, and does not extend to bind any act committed by a foreign party in foreign territory.

Under section 39(1)(d), the Commissioner may terminate or refuse to carry out an investigation if the relevant complaint does not satisfy any of the following conditions:

- either:
  - the complainant was resident in Hong Kong at the time that the relevant act or practice was done or engaged in; or
  - the data user was able to control, in or from Hong Kong, the collection, holding, processing or use of the personal data at the relevant time;
- the complainant was in Hong Kong at the relevant time; or
- the act or practice that is subject to the complaint may (in the Commissioner’s opinion) prejudice the enforcement of any right, or the exercise of any privilege, acquired or accrued in Hong Kong by the complainant.

The above is consistent with the Commissioner’s public comments in relation to this topic.

### 4 Key Principles

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

The PDPO is based on the following six Data Protection Principles (“DPP”) as set out in the PDPO:

DPP	Content
DPP1 – Data Collection Principle	Personal data must be collected in a lawful and fair way, for a purpose directly related to a function/activity of the data user. Data subjects must be notified of the purpose and the classes of persons to whom the data may be transferred. Data collected should be necessary but not excessive.
DPP2 – Accuracy and Retention Principle	Practicable steps shall be taken to ensure personal data is accurate and not kept longer than is necessary to fulfil the purpose for which it is used.

DPP	Content
DPP3 – Data Use Principle	Personal data must be used for the purpose for which the data is collected or for a directly related purpose, unless voluntary and explicit consent with a new purpose is obtained from the data subject.
DPP4 – Data Security Principle	A data user needs to take practicable steps to safeguard personal data from unauthorised or accidental access, processing, erasure, loss or use.
DPP5 – Openness Principle	A data user must take practicable steps to make personal data policies and practices known to the public regarding the types of personal data it holds and how the data is used.
DPP6 – Data Access and Correction Principle	A data subject must be given access to his/her personal data and allowed to make corrections if it is inaccurate.

The below sets out how key data protection principles are addressed under the PDPO:

Principle	How it is addressed in the PDPO?
Transparency	Under DPP5, a data user must publicly disclose its policies and practices in relation to personal data, including the types of personal data held by the data user and the main purposes for which personal data is used.
Lawful basis for processing	Under DPP3, except with the express and voluntary consent of the data subject, personal data may only be used for the original purpose for which it was collected or a directly related purpose.
Purpose limitation	DPP1 sets out that in relation to personal data collection: <ul style="list-style-type: none"> <li>■ Personal data must be collected for a lawful purpose that is directly related to a function or activity of the data user.</li> <li>■ Such collection must be necessary for or directly related to that purpose and not excessive in relation to that purpose.</li> <li>■ Personal data should be collected by lawful and fair means.</li> <li>■ A data user must provide certain information to the data subject when collecting the data subject's personal data (see "Individual Rights" below).</li> </ul>
Data minimisation	See DPP1 above.
Proportionality	See DPP1 above.
Retention	Under DPP2, data users must take all practicable steps to ensure that: <ul style="list-style-type: none"> <li>■ the personal data retained are accurate;</li> <li>■ the personal data are not retained for any longer than is necessary for the lawful purpose for which the data were collected; and</li> <li>■ when personal data are corrected that those corrections be provided to data users who were previously supplied the inaccurate data.</li> </ul> <p>If there are reasonable grounds for believing that personal data are inaccurate, data users should stop using the data.</p>

Principle	How it is addressed in the PDPO?
Security	See DPP4 above.
Data access and correction	A data subject has the right to ask a data user whether or not the data user holds any of his or her personal data, and to request a copy of such personal data held by that user. See also DPP6 above.

The PDPO sets out certain exemptions in relation to particular types/uses of personal data:

Exemption	Details
Exemptions from PDPO	If personal data are in any interception or surveillance product, or documents in relation to prescribed authorisation or device retrieval warrant governed by the Interception of Communications and Surveillance Ordinance.
Exemptions from all DPP, Parts 4 and 5 and sections 36 and 38(b)	If personal data are held for performing judicial functions or domestic or recreational purposes.
Exemption from DPP3	If personal data are required in legal proceedings or relates to: <ul style="list-style-type: none"> <li>■ the identity or location of a data subject and the applications of DPP3 would likely cause serious harm to an individual's health; or</li> <li>■ care and guardianship of minors.</li> </ul>
Exemptions from DPP6 and section 18(1)(b)	If personal data: <ul style="list-style-type: none"> <li>■ relate to employment decisions or certain incomplete decision-making processes;</li> <li>■ are held by the government to safeguard security, defence or international relations of Hong Kong;</li> <li>■ relate to criminal proceedings, misconduct or malpractice;</li> <li>■ are held for tax purposes;</li> <li>■ are held for discharging functions of a financial regulator; or</li> <li>■ relate to legal professional privilege claims.</li> </ul>
Exemptions from DPP3, DPP6 and section 18(1)(b)	If personal data relate to health of any individual or are used by the government to safeguard the security, defence or international relations of Hong Kong.



## 5 Individual Rights

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

Key right	Details
Right of access to data/copies of data	<p>Under DPP6, data subjects are entitled to:</p> <ul style="list-style-type: none"> <li>■ ascertain whether a data user holds any of their personal data (paragraph 6(a) of Schedule 1);</li> <li>■ request access to their personal data (paragraph 6(b) of Schedule 1); and</li> <li>■ request correction of any inaccuracies in their personal data (paragraph 6(e) of Schedule 1).</li> </ul> <p>Data access requests can be made by completing the prescribed form (from the Commissioner) and submitting it to the data user. There is no prescribed form for requesting corrections to personal data – such requests may be made in writing.</p> <p>A data user must respond to data access and correction requests within 40 days (sections 19(1) and 23(1)) or notify the data subject of reasons why the data user is unable to process the request within the prescribed time period.</p>
Right to rectification of errors	See “right of access to data” above.
Right to deletion/right to be forgotten	There is no general right to deletion or to be forgotten.
Right to object to processing	<p>There is no general right to object to processing.</p> <p>Under DPP3, data users may use or disclose personal data for:</p> <ul style="list-style-type: none"> <li>■ the original purpose for which the personal data were to be used at the time of collection;</li> <li>■ a purpose directly related to the original purpose of collection; or</li> <li>■ a purpose to which the data subject has given prescribed consent.</li> </ul>
Right to restrict processing	There is no general right to restrict processing.
Right to data portability	<p>There is no general right to data portability.</p> <p>When making a data access request, data subjects may request a copy of the relevant data in a specified form. The data user may provide the data in that specified form, or if it would not be reasonably practicable to do so, the data user may provide the data in another form.</p>

Key right	Details
Right to withdraw consent	<p>In relation to specific rights under the PDPO to withdraw consent (in addition for a data subject’s general right to withdraw consent):</p> <ul style="list-style-type: none"> <li>■ For personal data used for direct marketing, a data subject may at any time request a data user to cease using their personal data, regardless of whether the data is obtained directly from the data subject or not and whether an earlier consent has been given by the data subject to the data user or a third person for direct marketing. See question 9.1.</li> <li>■ “Prescribed consent” from the data subject is required under DPP3 if a data user intends to use the relevant personal data for a purpose other than the original purpose or a purpose directly related to the original purpose. The definition (under the PDPO) of prescribed consent means express consent of the data subject which has: <ul style="list-style-type: none"> <li>■ been voluntarily given; and</li> <li>■ not been withdrawn in writing.</li> </ul> </li> </ul>
Right to object to marketing	See question 9.1 and “right to withdraw consent” above.
Right to complain to the relevant data protection authority(ies)	Under section 37, a data subject who wants to lodge a complaint can do so in writing and in either Chinese or English.
Other key rights – please specify	<p>Under DPP1, a data user must explicitly or implicitly inform the data subject whether it is obligatory or voluntary for the data subject to supply the data and consequences for not supplying the data, and provide the name and address of the individual to whom any request to access and correct data may be made.</p> <p>See also section 4 above.</p>

## 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 under the PDPO.

There may be sector-specific requirements that are relevant to the handling or protection of personal data in those sectors. For example, the HKMA’s *Supervisory Policy Manual* (<http://www.hkma.gov.hk/eng/key-functions/banking-stability/supervisory-policy-manual.shtml>) contains guidelines in relation to outsourcing and technology risk management that apply to financial institutions who are regulated by the HKMA and which may have an impact on such organisation’s 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)?

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?**

This is not applicable in our jurisdiction.

**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 is optional in Hong Kong.

However, the Commissioner has published Guidance ([https://www.pcpd.org.hk/pmp/files/PMP\\_guide\\_e.pdf](https://www.pcpd.org.hk/pmp/files/PMP_guide_e.pdf)) that encourages organisations to appoint a Data Protection Officer.

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

This is not applicable in our jurisdiction.

**7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect to 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 the PDPO, if a data user engages a data processor (whether within or outside of Hong Kong) to process personal data on the data

user's behalf, the data user must adopt contractual or other means to prevent:

- any personal data transferred to the data processor from being kept longer than is necessary for processing of the data (DPP 2(3)); and
- any unauthorised or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing (DPP4(2)).

A data user remains liable for its agent's or contractor's breach.

Note that the PDPO does not:

- require a data user to first obtain a data subject's consent to transfer personal data before transferring to the data processor. In practice, data users will usually notify data subjects about such practice; and
- distinguish between related and unrelated entities.

The Commissioner has issued Guidance in relation to data users outsourcing processing of personal data ([https://www.pcpd.org.hk/english/publications/files/dataprocessors\\_e.pdf](https://www.pcpd.org.hk/english/publications/files/dataprocessors_e.pdf)) and engaging cloud computing service providers ([https://www.pcpd.org.hk/english/resources\\_centre/publications/files/IL\\_cloud\\_e.pdf](https://www.pcpd.org.hk/english/resources_centre/publications/files/IL_cloud_e.pdf)) – including in relation to the type of contractual means (whether entire agreement or additional clauses) that data users should consider entering into with data 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.)?**

---

See above.

## 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 PDPO has strict requirements in relation to direct marketing.

Under the PDPO, “direct marketing” is defined as the offering, or advertising of the availability, of goods, facilities or services or the solicitation of donations or contributions for charitable, cultural, philanthropic, recreational, political or other purposes, through direct marketing means. Note that direct marketing does not include communications that are not directed to a specific individual by name.

A data user must inform a data subject of the data user's intention to use the personal data in direct marketing, prior to such use. Specifically, a data user is required to inform data subjects of:

- its intention to use their personal data for direct marketing and that it can only do so with the data subject's consent;
- the types of personal data will be used for direct marketing;
- the classes of goods, facilities or services offered, or the purposes for which any donation or contribution is solicited; and
- the response channel through which the data subject may communicate the data subject's consent to the intended use.

The above information must be communicated to the data subject in a manner that is easily understandable and if in written form, easily readable. General descriptions of the types of goods offered

or the purposes of solicitation are not acceptable. In practice, one of the key issues in complying with direct marketing obligations is that the notification to data subjects must be sufficiently detailed with reference to the above points – general references to “certain products and services” are not sufficient to meet these requirements.

A data user must obtain consent of the data subject to the proposed direct marketing. As set out in the Commissioner's *New Guidance on Direct Marketing* ([https://www.pcpd.org.hk/english/publications/files/GN\\_DM\\_e.pdf](https://www.pcpd.org.hk/english/publications/files/GN_DM_e.pdf)), consent for direct marketing purposes includes an “indication of no objection” to the proposed use or provision. The “opt out” standard under the PDPO requires that data subjects explicitly indicate that their choice to opt out, for example, by signing and returning a form to the data user without checking the “opt out” box. Silence does not constitute consent.

If the data subject gives consent orally, the data user must send a written confirmation to the data subject within 14 days confirming the date of receipt of the consent and the scope of the consent obtained. When the data user uses the personal data in direct marketing for the first time, it must notify the data subject of its right to request the data user to stop using the personal data in direct marketing.

---

**9.2 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.)**

---

Under the *Unsolicited Electronic Messages Ordinance (Cap. 593)*, the Hong Kong Communications Authority established Do-not-call Registers to protect the public from receiving unsolicited commercial electronic messages sent to their telephone or fax numbers. There are Do-not-call Registers for fax, short messages and pre-recorded telephone messages.

In March 2018, the Hong Kong government released a consultation report ([http://www.cedb.gov.hk/ccib/eng/paper/pdf/Final-P2PCalls-ConsultationReport\(Eng\).pdf](http://www.cedb.gov.hk/ccib/eng/paper/pdf/Final-P2PCalls-ConsultationReport(Eng).pdf)) that proposes a statutory Do-not-call Register to be managed by the Commissioner – under this proposal, telemarketers may be subject to legal sanctions for calling those who have not given prior consent.

---

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

---

See question 3.1.

---

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

---

The direct marketing restrictions in the PDPO have been actively monitored and enforced by the Commissioner.

The Commissioner will, from time to time, make public announcements on its website in relation to its enforcement of the direct marketing restrictions. Such enforcement actions have resulted in enforcement notices (as referenced above) or in monetary penalties via Hong Kong courts.

The Commissioner has previously commented (in January 2018) on the direct marketing restrictions (in relation to a case ([https://www.pcpd.org.hk/english/news\\_events/media\\_statements/press\\_20180102b.html](https://www.pcpd.org.hk/english/news_events/media_statements/press_20180102b.html)) determined under the Magistrates' Court) as follows:

*“The Ordinance does not prohibit direct marketing activities. However, organisations must comply with the requirements of the Ordinance when carrying out direct marketing activities.*

*Organisations must obtain a data subject's consent before using his personal data in direct marketing. Appropriate training must be provided to its staff members to ensure their awareness of and compliance with the direct marketing provisions under the Ordinance."*

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

The Commissioner has given Guidance on the issue of using personal data from third parties for direct marketing purposes in its *New Guidance on Direct Marketing* ([https://www.pcpd.org.hk/english/publications/files/GN\\_DM\\_e.pdf](https://www.pcpd.org.hk/english/publications/files/GN_DM_e.pdf)).

If the data user plans to use the data received from a third party for direct marketing, the data user is required to follow the PDPO's direct marketing-related obligations, unless the third party confirms to the data user in writing that:

- the third party has given written notice to the data subject and obtained the data subject's written consent to the provision of personal data; and
- the use of the personal data is consistent with the consent obtained from the data subject.

Oral consent is not possible, and data users must disclose whether or not personal data has been transferred for gain. The above information must be communicated to the data subject in a manner that is easily understandable and if in written form, easily readable.

See question 9.1 for further details.

### 9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

Offence	PDPO section	Maximum fine (HK\$)	Maximum imprisonment
Using personal data in direct marketing without: (1) informing the data subject: (a) the data user intends to so use the personal data; (b) the data user may not so use the data unless with the data subject's consent; (c) the kinds of personal data to be used; and (d) the classes of marketing subjects which the data is to be used; and (2) providing the data subject with a response channel for the data subject to communicate consent without charge.	35C(5)	500,000	3 years

Offence	PDPO section	Maximum fine (HK\$)	Maximum imprisonment
Using personal data in direct marketing without: (1) having received the data subject's consent to the intended use; (2) having sent a written confirmation to the data subject within 14 days from receiving the consent if given orally, confirming: (a) the date of receipt of the consent; (b) the permitted kind of personal data; and (c) the permitted class of marketing subjects; and (3) ensuring the use of the personal data is consistent with the data subject's consent.	35E(4)	500,000	3 years
Failing to inform a data subject at the first time of using the personal data in direct marketing that the data user must, without charge, cease to use the data in direct marketing if the data subject so requires.	35F(3)	500,000	3 years
Failing to comply with the request to cease to use personal data in direct marketing made by a data subject without charge.	35G(4)	500,000	3 years



Offence	PDPO section	Maximum fine (HK\$)	Maximum imprisonment
<p>Failing to take any of the following actions before providing personal data to another person for direct marketing:</p> <p>(1) inform the data subject in writing:</p> <p>(a) the data user intends to so provide the personal data; and</p> <p>(b) the data user may not so provide the data unless with the data subject's written consent;</p> <p>(2) provide the data subject with written information in relation to:</p> <p>(a) where the data is to be provided for gain, that the data is to be so provided;</p> <p>(b) the kinds of personal data to be provided;</p> <p>(c) the classes of persons to which the data is to be provided; and</p> <p>(d) the classes of marketing subjects which the data is to be used; and</p> <p>(3) provide the data subject with a response channel through which the data subject may, without charge, communicate his consent to the intended use.</p>	35J(5)	<p>1,000,000 (for gain)</p> <p>500,000 (not for gain)</p>	<p>5 years (for gain)</p> <p>3 years (not for gain)</p>

Offence	PDPO section	Maximum fine (HK\$)	Maximum imprisonment
<p>Providing personal data to another person for direct marketing without:</p> <p>(1) having received the data subject's written consent to the intended provision of personal data;</p> <p>(2) if the data is provided for gain, having specified in the information provided to the data subject the intention to so provide; and</p> <p>(3) the provision of the data is consistent with the data subject's consent.</p>	35K(4)	<p>1,000,000 (for gain)</p> <p>500,000 (not for gain)</p>	<p>5 years (for gain)</p> <p>3 years (not for gain)</p>
<p>Failing to comply with a data subject's request to:</p> <p>(1) cease to provide the data subject's personal data for use in direct marketing; or</p> <p>(2) notify any data transferee in writing to cease to use the data in direct marketing.</p>	35L(6)	<p>1,000,000 (for gain)</p> <p>500,000 (in any other case)</p>	<p>5 years (for gain)</p> <p>3 years (in any other case)</p>
<p>A data transferee failing to comply with a data user's written notification to cease to use a data subject's personal data in direct marketing.</p>	35L(7)	500,000	3 years

## 10 Cookies

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

There is no Hong Kong law that specifically addresses the use of cookies. However, to the extent that cookies are used to store and collect personal data, the PDPO's relevant provisions would apply.

The Commissioner has published Guidance ([https://www.pcpd.org.hk/english/publications/files/guidance\\_internet\\_e.pdf](https://www.pcpd.org.hk/english/publications/files/guidance_internet_e.pdf)) that recommends websites that use cookies should explicitly state:

- the type of information that is stored in the cookies;
- whether that information may be transferred; and
- if so, to whom and for what purposes.

In addition, the Commissioner has published Guidance ([https://www.pcpd.org.hk/english/publications/files/online\\_tracking\\_e.pdf](https://www.pcpd.org.hk/english/publications/files/online_tracking_e.pdf)) on the use of online behavioural tracking tools in the context of PDPO compliance.

**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 our jurisdiction.

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

This is not applicable in our jurisdiction.

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

This is not applicable in our jurisdiction.

## 11 Restrictions on International Data Transfers

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

There are currently no restrictions in force regarding the transfer of personal data to other jurisdictions.

Section 33 of the PDPO sets out restrictions on the transfer of personal data to other jurisdictions, but it has not yet been enacted and is not operative. If and when it comes into effect, this section would prohibit data transfers to other jurisdictions unless certain conditions are met, including the requirements for the data user to obtain the data subject's written consent to the transfer and having reasonable grounds to believe that the personal data will be transferred to a jurisdiction that provides a degree of protection as the PDPO.

Section 33 was last discussed (<https://www.legco.gov.hk/yr16-17/english/panels/ca/papers/ca20170515cb2-1368-3-e.pdf>) in the Legislative Council Panel on Constitutional Affairs in May 2017. The Commissioner has also previously published Guidance ([https://www.pcpd.org.hk/english/resources\\_centre/publications/guidance/files/GN\\_crossborder\\_e.pdf](https://www.pcpd.org.hk/english/resources_centre/publications/guidance/files/GN_crossborder_e.pdf)) on cross-border data transfer under the PDPO (including model clauses) in December 2014. Some companies have taken the view of mitigating potential disruption by complying with this Guidance and section 33 in its operation (even though it is not yet operative).

**11.2 Please describe the mechanisms companies 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 not applicable in our jurisdiction.

**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 applicable in our jurisdiction.

## 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 on whistleblowing and there are no restrictions on the types of issues that may be reported. However, the following are relevant to this question:

- various measures exist in relation to the confidentiality of corruption reports to the police and the Hong Kong Independent Commission Against Corruption, with the objective of protecting anonymity and the personal safety of informers, ensuring immunity for witnesses and preventing unfair treatment; and
- section 30A of the *Prevention of Bribery Ordinance* prevents the names and addresses of informers from being used in civil or criminal proceedings.

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

There is no formal voluntary disclosure programme for claiming amnesty and reduced penalties, though a court and/or authorities may consider any such disclosures (on a case-by-case basis) in determining prosecution and/or penalties.

See 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)?**

The Commissioner has published Guidance ([https://www.pcpd.org.hk/english/resources\\_centre/publications/files/GN\\_CCTV\\_Drones\\_e.pdf](https://www.pcpd.org.hk/english/resources_centre/publications/files/GN_CCTV_Drones_e.pdf)) in relation to CCTV. This Guidance included the following information:

- The use of CCTV does not require separate registration/notification or prior approval from the PCPD.
- People should be explicitly informed that they are subject to CCTV surveillance.
- Data users are encouraged to conduct a privacy impact assessment before using CCTV – to help determine whether:
  - CCTV surveillance is appropriate;
  - there are any alternative means of achieving the same objective; and

- whether the data user can use the CCTV system responsibly and in compliance with the PDPO.
- A public notice is especially important for CCTV cameras that are discreetly placed or used in places where people may not expect to be under surveillance. The public notice should include details of the data user using the CCTV system, the purpose of conducting surveillance and contact details of the person to whom personal data privacy issues can be raised.

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

Pursuant to DPP3, personal data collected from CCTV surveillance should be deleted as soon as practicable after the purpose of collection is fulfilled.

## 14 Employee Monitoring

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

There are no specific rules on employee monitoring. To the extent that employee monitoring involves the collection, use and handling of personal data, it would be subject to the PDPO.

The Commissioner has published Guidance ([https://www.pcpd.org.hk/english/publications/files/monguide\\_e.pdf](https://www.pcpd.org.hk/english/publications/files/monguide_e.pdf)) on employee monitoring and personal data privacy in the workplace. The guidelines encourage: employers to evaluate the need for employee monitoring and how employee monitoring impacts the personal data privacy of employees; and offers practical advice on managing personal data obtained from employee monitoring.

In general, unless special circumstances exist, employee monitoring should be done in an overt manner. See question 14.2.

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

The Commissioner encourages employers to prepare an employee monitoring policy that states the purpose for employee monitoring, the circumstances under which employees may be monitored and the purpose for which personal data obtained from monitoring may be used. The employee monitoring policy should be communicated to employees and employers are responsible for safeguarding the protection of employees' personal data in monitoring records.

Consent to monitoring is not required. Consent to use of personal data obtained from monitoring is also not required unless the personal data is used for a purpose other than that stated in the Employee Monitoring Policy or a directly related purpose.

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

This is not applicable in our jurisdiction.

## 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 DPP4, data users must take all practicable steps to protect personal data having particular regard to:

- the kind of data and the harm that could result if any of those things should occur;
- the physical location where the data are stored;
- any security measures incorporated into any equipment in which the data are stored;
- any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and
- any measures taken for ensuring the secure transmission 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) expects voluntary breach reporting.

There is no mandatory data breach notification scheme under the PDPO. However:

- The Commissioner has published Guidance ([https://www.pcpd.org.hk/english/resources\\_centre/publications/files/DataBreachHandling2015\\_e.pdf](https://www.pcpd.org.hk/english/resources_centre/publications/files/DataBreachHandling2015_e.pdf)) on how to handle data breaches and breach notifications. In this Guidance, and in the event of a personal data breach:
  - the Commissioner recommends voluntary notification by the data user to the Commissioner. Specifically, the Commissioner notes that “*while it is not a statutory requirement on data users to inform the Office of the Privacy Commissioner for Personal Data, Hong Kong about a data breach incident concerning the personal data held by them, data users are nevertheless advised to do so as a recommended practice for proper handling of such incident*”; and
  - in relation to any notification to data subjects (where they can be identified), the Commissioner notes that “*a data user should consider notifying the data subjects and the relevant parties when real risk of harm is reasonably foreseeable in a data breach. Before making the decision, the consequences for failing to give notification should be duly considered*”.

The Commissioner has also published a template ([https://www.pcpd.org.hk/english/publications/files/NotificationForm\\_e.pdf](https://www.pcpd.org.hk/english/publications/files/NotificationForm_e.pdf)) data breach notification form, which a data user may use to report a data breach to the Office of the Privacy Commissioner for Personal Data.

- Regulators in certain industries (e.g. financial institutions) may require entities that they regulate to notify data subjects of any data 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) expects voluntary breach reporting.**

See question 15.2.

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

Offence	Maximum fine (HK\$)	Maximum imprisonment
Contravention of an enforcement notice	50,000	2 years
Contravention of provisions of PDPO (other than as set out in this table)	10,000	6 months
Direct marketing-related offences	See question 9.6	

## 16 Enforcement and Sanctions

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

See also question 15.4.

The Commissioner can investigate complaints regarding PDPO breaches and initiate investigations. There is scope for criminal enforcement and penalties for non-compliance in certain circumstances.

The Commissioner will first contact the complainant (and potentially the alleged offending data user) to determine if a formal investigation should be undertaken. If the Commissioner commences an investigation and finds that the alleged offender has breached the PDPO, the Commissioner may serve an enforcement notice that directs the offender to take certain steps to remedy the contravention.

Breaching an enforcement notice is an offence under section 50A. The Commissioner can institute civil or criminal proceedings against any data user that breaches an enforcement notice, and can also publish results of any investigation (including naming the data user involved and details of the breach).

In addition to the above, section 66 also provides that a complainant may seek compensation directly from the relevant data user.

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
<p>The Commissioner may investigate all contraventions of the PDPO, including breaches of the DPPs. The Commissioner may initiate investigations either after receiving a complaint submitted by a data subject under section 37 or on its own initiative.</p> <p>After completing an investigation, the Commissioner may choose to publish a report setting out the investigation results and any recommendations or comments from the investigation.</p> <p>Note that the Commissioner receives a large amount of enquiries and cases each year and carries out a number of investigations; many cases are resolved without the need for the Commissioner to issue an enforcement notice.</p>	<p>The Commissioner may issue an enforcement notice if the Commissioner is reasonably satisfied that the contravention is continuing or likely to be repeated. The data user may make an appeal against an enforcement notice to the Administrative Appeals Board within 14 days. Non-compliance with an enforcement notice is a criminal offence.</p> <p>The Commissioner may provide legal assistance to an aggrieved data subject who institutes proceedings against a data user seeking compensation for damaged suffered by reason of the data user's contravention of the Ordinance. The Commissioner has no power to order compensation.</p>	<p>The Commissioner has no power to impose criminal sanctions but may refer criminal offences under the PDPO to the Hong Kong Police. Any such matters may then be prosecuted via the Hong Kong court system.</p>

**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 in our jurisdiction.

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

This is not applicable in our jurisdiction.

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

See question 3.1.

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

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

Companies generally comply with such requests, subject to any prohibitions under Hong Kong law (e.g. secrecy obligations in the *Securities and Futures Ordinance (Cap. 571)*, prohibiting any persons assisting the Securities and Futures Commission in carrying out their investigations from disclosing anything about the investigation to anyone).

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

The Commissioner has not issued any specific Guidance on e-discovery or 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.

In 2017 ([https://www.pcpd.org.hk/english/news\\_events/whatison/files/ca20180214cb2\\_851\\_3\\_e.pdf](https://www.pcpd.org.hk/english/news_events/whatison/files/ca20180214cb2_851_3_e.pdf)), the PCPD received:

- 15,594 enquiries – representing a decrease of 3.6% from 2016 (16,180 enquiries received); and
- 3,501 complaints – representing an increase of 90% from 2016 (1,838 complaints received). This increase was largely linked to the reported loss of two laptops by the Registration and Electoral Office (there were 1,968 complaints related to this incident).

As above, enforcement of the PDPO's direct marketing provisions continues to be a focus for the Commissioner. For example, PARKnSHOP (HK) Limited was convicted and fined HK\$3,000 in January 2018 for sending direct marketing materials without obtaining the data subject's consent. This is the first conviction under section 35E(1) since the amendment provisions on direct marketing came into effect in April 2013.

The Commissioner has also commented ([https://www.pcpd.org.hk/english/news\\_events/media\\_statements/press\\_20180412.html](https://www.pcpd.org.hk/english/news_events/media_statements/press_20180412.html)) that accountability and data ethics are essential solutions to help regulators strengthen regulatory effectiveness and businesses to unlock innovative use of data in the data-driven economy.

See also question 18.2.

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

We have identified several areas of focus throughout this chapter.

In general, the Commissioner's public comments have indicated that it is increasingly proactive in relation to the PDPO and its enforcement – this has been ongoing since the Commissioner's release (in February 2014) of the *Privacy Management Programme – A Best Practice Guide* ([https://www.pcpd.org.hk/pmp/files/PMP\\_guide\\_e.pdf](https://www.pcpd.org.hk/pmp/files/PMP_guide_e.pdf)), which encouraged organisations to (in addition to legal requirements) proactively embrace data protection as part of their corporate governance responsibilities.

In particular:

- The Commissioner has commented that it is currently reviewing how the GDPR and other international privacy legislations (including the APEC Cross Border Privacy Rules) align with the PDPO. In April 2018, the Commissioner issued the European Union General Data Protection Regulation ("GDPR") 2016 booklet, in order to prepare businesses for the GDPR that will come into force on 25 May 2018. The GDPR explicitly requires compliance by organisations established in non-EU jurisdiction in certain situations. Compliance with the GDPR is an increasing area of concern for Hong Kong-based organisations.

- As the use of drones is increasingly prevalent, the Commissioner reiterated the importance of compliance with the PDPO should collection of personal data be involved, and the Commissioner will submit recommendations to the government on regulation of drones from the personal data protection perspective.
- Both the Commissioner and industry regulators have been paying increasing attention to cybersecurity-related issues and initiatives. For example:
  - in December 2016, the HKMA announced a new Cyber Fortification Initiative to improve the cyber resilience of its Authorised Institutions; and
  - in October 2017, the SFC issued guidelines (<https://sfc.hk/edistributionWeb/gateway/EN/news-and-announcements/news/doc?refNo=17PR133>) and baseline requirements for licensed or registered persons engaged in internet trading, to enhance cybersecurity and mitigate hacking risks.
- Following recent cyberattacks and personal data leaks, the Commissioner has commented (<http://www.scmp.com/news/hong-kong/community/article/2143156/hong-kongs-privacy-commissioner-review-ageing-data>) (in April 2018) that it will look to review the PDPO, with reference to whether enough protection was provided to citizens and global trends, as well as potentially increasing enforcement powers and penalties. This aligns with the Commissioner's release of its Guidance in relation to the GDPR (see above).

More generally, in relation to the PCPD's goals going forward, the PCPD has commented ([https://www.pcpd.org.hk/english/news\\_events/whatison/files/ca20180214cb2\\_851\\_3\\_e.pdf](https://www.pcpd.org.hk/english/news_events/whatison/files/ca20180214cb2_851_3_e.pdf)) that:

*"The PCPD notices that the privacy protection landscape is rapidly changing with ICT developments and digitalisation of our economy... PCPD will proactively assist local data users in understanding and complying with data protection regimes overseas, and duly consider the need to establish a comparable framework and mechanism interoperable with international data protection authorities without compromising economic and ICT development.*

*In 2018, the PCPD will take proactive steps to strike the balance between privacy protection and free flow of information, and look closely into the use of ethical framework as an innovative solution to regulate these new disruptive technologies. Special focus will be placed on:*

- *Engaging the business sector (especially the micro, small and medium size enterprises) in promoting the protection and respect of personal data privacy, with a view to enhancing the culture of respect of personal data privacy in the sector;*
- *Strengthening the working relationship with the Mainland and overseas data protection authorities, and explaining the newly implemented rules and regulations on data protection of other jurisdictions to the local stakeholders for compliance with the requirements; and*
- *Providing advice to the Government on initiatives involving personal data privacy."*



**Joshua Cole**

Ashurst Hong Kong  
11/F Jardine House  
1 Connaught Place  
Hong Kong

Tel: +852 2846 8989  
Email: [joshua.cole@ashurst.com](mailto:joshua.cole@ashurst.com)  
URL: [www.ashurst.com](http://www.ashurst.com)

Joshua is Managing Partner of the Ashurst Hong Kong office and leads our Digital Economy practice in Asia.

Joshua has over 20 years of experience advising on TMT and related corporate and commercial matters, to clients in TMT and other sectors – including financial services, energy and resource, pharmaceutical and retail. He has advised on a number of high-profile international acquisitions, disposals and joint ventures involving Hong Kong, China, Japan, Myanmar, Korea, the Philippines and other South East Asian countries. He also advises telecommunications businesses on commercial and regulatory matters in Asia, including network build agreements and spectrum acquisitions/licensing.

Joshua has been named by *Chambers Asia Pacific* as a leading TMT lawyer, and is the author of various M&A and telecommunications law-related publications.

**Hoi Tak Leung**

Ashurst Hong Kong  
11/F Jardine House  
1 Connaught Place  
Hong Kong

Tel: +852 2846 8982  
Email: [hoitak.leung@ashurst.com](mailto:hoitak.leung@ashurst.com)  
URL: [www.ashurst.com](http://www.ashurst.com)

Hoi is Counsel in the Ashurst Hong Kong office.

Hoi brings a wealth of experience on technology and IP-related matters across Asia. He has advised a broad spectrum of clients from multinational corporations to start-ups, spanning from TMT to other sectors such as financial services, insurance, entertainment, education and retail. His practice includes advising on:

- transaction structuring, contract drafting and negotiations – including: outsourcing, procurement, supply and distribution arrangements; technology and content licensing, use and development; launch/expansion of B2B and B2C technology services; cloud computing, data centre and telecommunications/network infrastructure projects; and BAU commercial agreements;
- TMT/IP/data-focused corporate transactions – including: M&As; JVs; and restructurings; and
- TMT-related issues – including: fintech; cryptocurrencies; cybersecurity; data privacy and big data arrangements; and emerging technologies and businesses (e.g. blockchain, smart contracts, artificial intelligence and e-sports) in various industry sectors.

Hoi works closely with the Ashurst Advance team – with a particular interest in legal service innovation through technology (including automation of legal tasks and smart contracts). He writes frequently, and is regularly quoted by the media on technology law-related topics.

Ashurst is a leading global law firm with a rich history spanning almost 200 years. Our in-depth understanding of our clients and commitment to providing exceptional standards of service have seen us become a trusted adviser to local and global corporates, financial institutions and governments on all areas of commercial law.

Our people are our greatest asset. We bring together lawyers of the highest calibre with the technical knowledge, industry experience and regional know-how to provide the inclusive advice our clients need.

We currently have 25 offices in 15 countries and a number of referral relationships that enable us to offer the reach and insight of a global network, combined with the knowledge and understanding of local markets. With over 400 partners and a further 1,450 lawyers working across 10 different time zones, we are able to respond to our clients wherever and whenever they need us.

Our clients value us for being approachable, astute and commercially minded. As a global team, we have a reputation for successfully managing large and complex multi-jurisdictional transactions, disputes and projects, and delivering outstanding outcomes for clients.

# India

Hari Subramaniam



Aditi Subramaniam



## Subramaniam & Associates (SNA)

### 1 Relevant Legislation and Competent Authorities

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

In the absence of specific legislation, data protection is achieved in India on the basis of the following legislation, which applies also to other aspects of online regulations, such as e-commerce and cybercrime:

- **The Information Technology Act (2000), amended by the Information Technology (Amendment) Act (2008)** – henceforth referred to as the IT Act – which contains provisions for the protection of electronic data. The IT Act penalises “cyber contraventions” which attract civil prosecution under section 43 (a)–(h) and “cyber offences” which attract criminal action under sections 63–74. The former category includes gaining unauthorised access to, and downloading or extracting data from, computer systems or networks. The latter covers “serious” offences like tampering with computer source code, hacking with intent to cause damage and breach of confidentiality and privacy.

In April 2011, the Indian Ministry of Communications and Technology published four sets of rules implementing certain provisions of the Information Technology (Amendment) Act (2008), as follows:

- The Security Practices Rules require entities holding sensitive personal information of users to maintain certain specified security standards.
- The Intermediary Guidelines Rules prohibit content of specific nature on the internet. An intermediary, such as a website host, is required to block such content.
- The Cyber Café Rules require cyber cafés to register with a registration agency and maintain a log of the identity of users and their internet usage.
- Under the Electronic Service Delivery Rules, the Government can specify certain services, such as applications, certificates, licences, etc., to be delivered electronically.

Of relevance to the issue of data protection is the first set of rules in the list above:

- **The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules (2011)** – henceforth referred to as the IT Rules – which were framed under section 43A of the IT Act. The IT Rules set out procedures for corporate entities which collect, process or store personal data (including sensitive personal information). These Rules also distinguish “personal information” from “sensitive personal information”.

It must be pointed out that because the statutes in question were not drafted specifically with the protection of data in mind, the assortment of existing legislation currently being used for this purpose leaves a lot to be desired in terms of effective protection of data and even a basic definition of scope and sanctions.

The Government recognises this, and has also proposed to enact specific legislation on privacy (the Privacy Bill) which, if it comes into force, will override the IT Rules. The Privacy Bill recognises an individual’s right to privacy and provides that this right cannot be infringed except in certain circumstances specified in the Bill, which include the protection of national integrity or sovereignty, national security, prevention of crime and public order. Although the Privacy Bill was first drafted in 2011, and multiple revised drafts have been published regularly ever since, the Bill has not yet passed into Law. Currently, two major issues are hindering smooth passage of the Bill in the Legislature:

- 1) A disagreement between the judiciary and intelligence agencies over whether or not the agencies ought to be under the scrutiny of a competent court with respect to interception of personal data when they deem it necessary.
- 2) A debate over the extension of protection granted by the legislation to all residents of the country (as opposed to only the citizens).

The Bill was expected to become law by the end of 2016, but this has not yet materialised. It must be noted that although the latest draft of the proposed Bill was allegedly circulated to the Committee of Secretaries and leaked to the Centre for Internet and Society (an independent non-profit organisation in Delhi and Bangalore) in 2014, this last draft is not yet publicly available. All references to the draft Privacy Bill in this chapter therefore refer to the publicly available draft from 2011.

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

Apart from the Privacy Bill, 2011, a Data (Privacy and Protection) Bill, 2017 (Data Privacy Bill, 2017) had been introduced in the parliament in July 2017 by a private member. Apart from intending to make Right to Privacy a statutory right and streamlining the data protection regime in India, it seeks the establishment of a Data Privacy and Protection Authority for regulation and adjudication of privacy-related disputes. It is yet to be enacted into law.

Data protection may also sometimes occur through the following:

- **The Copyright Act (1957):** Since the Act protects intellectual property rights in different types of creative work including literary works, and the term “literary work” statutorily includes computer databases, copying a computer

database, or copying or distributing, a database could amount to copyright infringement under the Act. This provides some scope for protecting different types of data as “literary works”. Obviously, however, there is a difference between database protection and data protection. Database protection protects the creative investment in compilation, presentation and verification of databases, while data protection aims to protect the privacy of individuals by limiting or restricting access to their personal or sensitive information.

- **The Indian Penal Code (1860):** This could be used to prevent theft of data. The offences of theft and misappropriation technically apply only to movable property under the Indian Penal Code, but the term “movable property” has been defined to include corporeal property of every description except land or property that is permanently attached to the earth.
- **The Indian Constitution:** Article 21 of the Constitution protects an individual’s right to life and personal liberty. The Supreme Court of India in a nine-judge bench decision in August 2017 held that citizens enjoy a fundamental right to privacy that it is intrinsic to life and liberty. The 2014 draft of the Privacy Bill recognises the right to privacy as being under the scope of Article 21 of the Constitution. Article 300A of the Constitution also guarantees the right not to be deprived of one’s property except by authority of law, so if the data in question is regarded as property, this provision may be relied upon. It must be noted, however, that rights guaranteed by the Constitution may normally only be used against the State or State-owned enterprises.

In addition to the above, invasion or breach of privacy could lead to an action in tort.

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

Business Process Outsourcing Units implement self-regulatory processes, such as the BS 7799 and the ISO 17799 standards, to standardise information security management and restrict the quantity of data made available to employees.

The Reserve Bank of India periodically issues guidelines, regulations and circulars to maintain the confidentiality and privacy of client information, and in 2006, in conjunction with several other banks belonging to the Indian Banks Association, also established a body called the Banking Codes and Standards Board of India to evolve a set of voluntary norms which banks must enforce themselves through internal grievance redressal mechanisms within each bank. These mechanisms include a designated “Code Compliance Officer” and an Ombudsman.

The Medical Council of India has set out the Indian Medical Council (Professional conduct, Etiquette and Ethics) Regulations, 2002 (Code of Ethics Regulations, 2002). These rules govern various issues, including doctor-patient confidentiality, the collection of personal data from patients, issues of consent, and the extent to which invasive procedures may be conducted.

Similarly, the Securities and Exchange Board of India is a securities market regulator which requires securities market intermediaries to maintain confidentiality of client data, including personal data.

These regulations apply in addition to the IT Rules. While they provide a certain degree of security, the lack of legislative enforcement and foresight mean that they are enforced in varying degrees by each individual institution and do not come with guaranteed parliamentary sanction.

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

There are no specific national regulators dealing with the administration

of privacy laws in India. However, the proposed Privacy Bills contemplate the creation of a Data Protection Authority of India which will monitor and enforce the proposed laws.

In cases where the compensation amount claimed for a failure to protect confidentiality of sensitive personal information is less than INR 50,000,000, the IT Act provides for the Government to appoint an Adjudicating Officer. All proceedings before the Adjudicating Officer are deemed to be judicial proceedings and the officer has the powers of a civil court. The details of the enquiry procedure that the Adjudicating Officer must use are provided in the Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules (2003).

## 2 Definitions

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

#### ■ “Personal Data”

The legislation does not contain a definition of the term “personal data”. However, the IT 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 a person.

The IT Act defines “data” as a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts, magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.

The draft of the proposed Privacy Bill, 2011 defines “personal data” as any data which relates to a living, natural person, if that person, either directly or indirectly, in conjunction with other data that the data controller has or is likely to have, can be identified from that data. This includes any expression of opinion about said person.

#### ■ “Processing”

Neither the IT Act nor the IT Rules contain a definition of the term “processing”.

However, the proposed Privacy Bill defines processing as any operation, or set of operations, whether carried out through automatic means or not, that relate to:

1. the organisation, collation, storage, update, modification, alteration or use of personal data; or
2. the merging, linking, blocking, degradation, erasure or destruction of personal data.

The proposed Privacy Bills define processing as obtaining or recording the information or data or carrying out any operation or set of operations on the information or data, whether or not by automatic means, including:

- (i) organisation, adaptation or alteration of the information;
- (ii) or data;
- (iii) retrieval, consultation or use of the information or data;
- (iv) disclosure of the information or data by transmission, dissemination or otherwise making available; or
- (v) alignment, combination, blocking, erasure or destruction of the information or data.

#### ■ “Controller”

Neither the IT Act nor the IT Rules contain a definition of the term “data controller”.

However, the proposed Privacy Bill, 2011 defines the term as any person who processes personal data. This includes bodies corporate, partnerships, societies, trusts, associations of persons, Government companies, Government departments, urban local bodies, agencies or instruments of the State.

Additionally, the proposed Data Privacy Bill, 2017 defines the term as a person who, either alone or jointly or in combination with other persons, determines the purposes for which and the manner in which any personal data are used, or are to be, processed.

#### ■ “Processor”

Neither the IT Act nor the IT Rules contain a definition of the term “data processor”.

However, the proposed Data Privacy Bill, 2017 defines the term as any person, apart from an employee of a data controller, who processes data independently or on behalf of a data controller.

#### ■ “Data Subject”

In August 2011, the Ministry of Communications and Information issued a “Press Note” (Clarification on the Privacy Rules) which states that the term “provider of information” refers to those natural persons who provide sensitive personal data or information to a body corporate. It is generally understood that “provider of information” is synonymous with “data subject”, although the legislation contains no definition of either term.

According to the proposed Privacy Bill, 2011, a data subject is any living individual whose personal data are processed by a data controller in India.

#### ■ “Sensitive Personal Data”

The IT Rules define “sensitive personal data or information” as such personal information which consists of information relating to:

- passwords;
- financial information, such as bank account or credit card or debit card or other payment instrument details;
- physical, physiological and mental health conditions;
- sexual orientation;
- medical records and history;
- biometric information;
- any details relating to the above clauses as provided to a body corporate for provision of services; and
- any information received under the above clauses by a body corporate for processing, or which has been stored or processed under lawful contract or otherwise.

Provided that any information that is freely available or accessible in the public domain, or furnished under the Right to Information Act (2005) or any other law currently in force, shall not be regarded as sensitive personal data or information for the purposes of these rules.

The proposed Privacy Bill, 2011 and Data Privacy Bill, 2017 provide a more specific definition of “sensitive data” as follows:

“Sensitive personal data” of an individual means personal data relating to:

1. Unique Identifiers such as the Aadhar number or PAN (Personal Account Number);
2. physical and mental health, including medical history;
3. biometric or genetic information;
4. criminal convictions;
5. banking credit and financial data; and
6. narco analysis and/or polygraph test data.

#### ■ “Data Breach”

Neither the IT Act nor the IT Rules contain a definition of the term “data breach”.

However, according to the Data Privacy Bill, 2017, Data Breach includes any unauthorised access, destruction, use, processing, storage, modification, de-anonymisation, unauthorised disclosure (either accidental or incidental) or other reasonably foreseeable risks or data security breaches of personal data.

#### ■ Other key definitions – please specify (e.g., “Pseudonymous Data”, “Direct Personal Data”, “Indirect Personal Data”)

##### ■ “Pseudonymous Data”

Neither the IT Act nor the IT Rules contain a definition of the term “pseudonymous data”.

##### ■ “Direct Personal Data”

Neither the IT Act nor the IT Rules contain a definition of the term “direct personal data”.

##### ■ “Indirect Personal Data”

Neither the IT Act nor the IT Rules contain a definition of the term “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, section 75 of the IT Act states that the provisions of the Act would apply to any offence or contravention thereunder committed outside India by any person (including companies), irrespective of his nationality, if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

## 4 Key Principles

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

#### ■ Transparency

Under the IT Rules, data controllers and data processors must provide a privacy policy for the handling of or dealing in personal information, including sensitive personal information, and ensure that this policy is available to the data subject who has provided said information by lawful contract. Further, the policy shall be published on the website of the body corporate or any person on its behalf, and shall provide:

1. clear and easily accessible statements of the practices and policies of the data controller;
2. types of sensitive or personal data or information collected by the body corporate and as defined by the IT Rules;
3. the purpose of collection and usage of such information;
4. disclosure of information including sensitive personal data or information as and when it is requested by the data subject under specified conditions; and
5. reasonable security practices and procedures as specified in the Rules.

The proposed Privacy Bill, in Chapter III, section 9, further provides for the following principles to be adhered to in the transparent collection of personal data:

Personal data must be directly collected from the data subject except if:



1. the information is part of the public record or has been made public by the data subject; or
2. the data subject has consented to the collection of personal data from another source.

Further, the Bill also states that when personal data are collected directly from the data subject, the data controller must, at any time before the data are processed, take reasonable steps to make the data subject aware of the following:

1. the documented purpose for which such personal data are being collected;
2. whether provision of data by the data subject is voluntary or mandatory under the law, or simply in order to avail of any products or services;
3. the consequences of the failure to provide said personal data;
4. the recipient or category of recipients of the personal data;
5. the name and address of the data controller and all persons who are, or will be, processing information on behalf of the data controller; and
6. if it is intended that the personal data be transferred out of the country, the details of said transfer.

#### ■ Lawful basis for processing

- The IT Rules mandate that the body corporate (or any person on its behalf) must obtain consent in writing from the data subject for the specific purpose for which the data will be used, before the collection of the data. Sensitive personal information may only be collected for a lawful purpose connected with a function or purpose of the corporate entity, and only if such collection is considered necessary for that purpose. The corporate entity must ensure that the information is being used only for the purpose for which it was collected.
- The proposed Privacy Bill, 2011 further provides that personal data shall be collected only with the consent of the data subject, unless said collection is either necessary for the data controller in order to comply with a particular law or ordinance, or is mandatory under current law. However, for any data subject under the age of 18, obtaining consent from their legal or natural guardian is mandatory, regardless of the exceptions previously made.
- The Bill also provides, in sections 9 and 10 of Chapter III, guidelines for the lawful processing of personal data, specifying that personal data must be processed only in a fair, appropriate and lawful manner and for the documented purpose alone. The Bill states that the data controller shall collect and process only such type and amount of personal data as is absolutely necessary to fulfil the documented purpose. Data controllers must also ensure, according to the Bill, that all persons involved in any stage of the processing of personal data shall treat the personal data as confidential, and shall communicate said data only with people who are directly employed by the data controller, or any sub-contractor of the data controller who is under an obligation to maintain confidentiality.
- The drafters of the proposed Privacy Bill, 2011 have also seen fit to draw a distinction between the guidelines for the lawful processing of personal data and those that govern the processing of sensitive personal data. Chapter III, section 12 of the Bill specifically addresses the processing of sensitive personal data, stating that it shall not be collected or processed “unless authorised by authority”, further stating that “no such authorisation shall be required” in a particular list of circumstances, which include, among other things, that the collection or processing of such data is required by law, the said data has already been made public

by the data subject, such collection and processing is made in connection with any legal proceedings if said processing is necessary for the purposes of obtaining legal advice, or for establishing or defending legal rights, and if data relating to criminal conviction, biometrics and genetic information is collected and processed by law enforcement agencies.

#### ■ Purpose limitation

The IT Rules or the Act do not provide a specific time frame for the retention of sensitive personal information. However, the IT Rules state that a body corporate or any person on its behalf holding sensitive personal data or information shall not retain that information for longer than is required for the purposes for which the information may lawfully be used or is otherwise required under any other law for the time being in force.

#### ■ Data minimisation

There is no statutory definition or guidance with respect to data minimisation.

#### ■ Proportionality

There is no statutory definition or guidance with respect to proportionality.

#### ■ Retention

As explained above, neither the IT Rules nor the IT Act provides specific guidance with respect to the time frame for retention of sensitive personal information. However, the Rules do not override provisions of other laws that may specify a maximum period of retention for sensitive data. For example, telecom licences require licensees to maintain, for security reasons and for scrutiny by the Department of Telecommunication, all commercial records related to communications exchanged on the network for at least one year.

Section 67 C of the IT Act requires an intermediary to retain such information, and for such period of time as shall be prescribed by the Central Government. “Intermediary” includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online auction sites, online marketplaces and cyber cafés. The Central Government has yet to frame rules implementing the retention provision, and therefore the nature of data to be retained and the duration of retention are unclear.

The proposed Privacy Bill, 2011 will clarify the law on retention of personal data, stating as it does in section 13 of Chapter II that personal data shall only be retained for as long as is necessary to achieve the documented purpose, unless:

1. it is required by law to be retained for a longer period;
2. the data subject consents to its retention for a longer period;
3. such retention is required by a contract between the data subject and the data controller; or
4. it is required to be so retained for historical, statistical or research purposes.

The Bill further states that all personal data that need no longer be retained in accordance with the above shall either be destroyed or anonymised. During the process of destruction or anonymisation, the data controller must ensure that unauthorised persons do not gain access to the personal data. The destruction of personal data must be carried out in a manner that ensures that it is impossible to re-identify the personal data once it has been destroyed.

#### ■ Other key principles – please specify

There are no other key principles in particular.



## 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

Rule 5, subsection 6 of the IT Rules mandates that the body corporate or any person on its behalf must permit providers of information or data subjects to review the information they may have provided. However, the Rules do not explain the procedure to be followed by data subjects in exercising the right to access the data they have provided. It also does not detail whether there is a time limit within which the data processor must comply with a request for access.

This situation will be clarified somewhat by the proposed Privacy Bill, which states that any data subject shall, provided he or she can prove her identity, have the right to ask for confirmation from the data controller has complete control over the personal data, request details with respect to who else – including any third parties – has access to the personal data, and require the data controller to provide information about the logic involved in the automated process of decision-making where the personal data in question is being processed automatically for evaluation purposes.

The Bill states that data controllers must provide the required information to the data subject within 45 days of receiving a request for it, provided that the request was accompanied by the prerequisite fee, and that the data controller is obliged to inform the data subject that the latter may legally ask the data controller to make any changes to inaccurate or deficient personal data. Access to personal data may be denied only if the information cannot be given out without also disclosing information about another data subject who could be identified from that information, unless that data subject has consented to such disclosure.

#### ■ Right to rectification of errors

This is the same as the “right to deletion/right to be forgotten”; see below.

#### ■ Right to deletion/right to be forgotten

Rule 5, subsection 6 of the IT Rules states that data subjects must be allowed access to the data provided by them and ensure that any information found to be inaccurate or deficient shall be corrected or amended as feasible. Although the Rules do not directly address deletion of data, they state in Rule 5, subsection 1, which corporate entities or persons representing them must obtain written consent from data subjects regarding the usage of the sensitive information they provide. Further, data subjects must be provided with the option not to provide the data or information sought to be collected.

The proposed Privacy Bills affirm the above, and further states that unless the data controller can adduce adequate evidence of the complete accuracy and completeness of the data and the fact that it is entirely fitting with respect to the purpose of the data collection in question, or of the lawfulness of its collection, the data subject has the right to request a data controller to destroy any personal data that he or she considers either excessive in relation to the documented purpose of collection, or based on incorrect facts, or processed unlawfully.

The Supreme Court of India in a nine-judge bench decision in August 2017 also identified the right to be forgotten, in physical and virtual spaces such as the internet, under the umbrella of informational privacy.

#### ■ Right to object to processing

Rule 5 of the IT Rules states that the data subject or provider of information shall have the option to later withdraw consent which may have been given to the corporate entity previously; such withdrawal of consent must be stated in writing to the body corporate. On withdrawal of consent, the body corporate is prohibited from processing the personal information in question.

In the case of the data subject not providing consent, or later withdrawing consent, the body corporate shall have the option not to provide the goods or services for which the information was sought.

#### ■ Right to restrict processing

The proposed Data Privacy Bill, 2017 states that during the pendency of request for removal of specific personal data, the Data Controller and Data Processor shall restrict processing of the specific personal data of the person but it shall not restrict the collection or storage of personal data.

#### ■ Right to data portability

The proposed Data Privacy Bill, 2017 states that every person shall, as and when required, receive the personal data concerning him, which he has provided to a data controller, in a structured, commonly used and machine-readable format and have the right to data portability to another data controller without any hindrance.

#### ■ Right to withdraw consent

The proposed Data Privacy Bill, 2017 envisages the right to seek removal of personal data from the data controller where a person has withdrawn his consent.

#### ■ Right to object to marketing

This is the same as the “objection to processing”; see above.

#### ■ Right to complain to the relevant data protection authority(ies)

Rule 5, subsection 9 of the IT Rules mandates that all discrepancies or grievances reported to data controllers must be addressed in a timely manner. Corporate entities must designate Grievance Officers for this purpose, and the names and details of said officers must be published on the website of the body corporate. The Grievance Officer must redress respective grievances within a month from the date of receipt of said grievances.

The proposed Privacy Bills also seek establishment of a Data Privacy and Protection Authority for regulation and adjudication of privacy-related complaints and disputes.

#### ■ Other key rights – please specify

##### Disclosure of data

Data subjects also possess rights with respect to disclosure of the information they provide. Disclosure of sensitive personal information requires the provider’s prior permission, unless either:

1. disclosure has already been agreed to in the contract between the data subject and the data controller; or
2. disclosure is necessary for compliance with a legal obligation.

The exceptions to this rule are if an order under law has been made, or if a disclosure must be made to Government agencies mandated under the law to obtain information for the purposes of:

1. verification of identity;
2. prevention, detection and investigation of crime; or
3. prosecution or punishment of offences.

Recipients of this sensitive personal information are prohibited from further disclosing said 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 are no statutory registration or notification requirements for either data processors or data controllers.

The proposed Privacy Bills provides for the establishment of a Data Protection Authority of India, and in Chapter VII, section 43, stipulates that the Authority shall establish and maintain a National Data Controller Registry – “an online database to facilitate the efficient and effective entry of particulars by data controllers”. If the Bill is enacted, data controllers shall not be permitted to process any data belonging to any data subject for a given documented purpose, unless they first make an entry in the Registry in a format to be pre-ordained by the Central Government.

### 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 answer is the same as the answer to 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)?

India has no current legislative requirements with respect to registration or notification. However, the draft of the proposed Privacy Bills suggests that the registration requirements it prescribes, once enforced, will function as per the documented purpose 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)?

The legislation currently in force in India contains no information on registration requirements for data processors or controllers. However, the proposed Privacy Bills state that all data controllers who wish to process data for a particular purpose must first register with the National Data Controller Registry with respect to that particular documented purpose.

### 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)?

As stated in questions 6.1, 6.3 and 6.4 above, India currently does not have any legislative requirements with respect to registration or notification procedures for data controllers or processors. However, the proposed Privacy Bill, 2011 prescribes in Chapter VII, section 43(5) that the National Data Controller Registry shall contain the following details of data controllers in respect of each documented purpose for which the personal data is being processed:

1. name;
2. address of principal place of business of the data controller;
3. name and address of the nominated representative of the data controller if one has been so nominated;
4. description of the documented purpose;
5. description of the personal data being processed or to be processed by the data controller;
6. description of the recipients of the personal data or any persons to whom the data controller may disclose the personal data; and
7. description of the countries to which the data controller directly or indirectly transfers or intends to transfer the personal data.

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

Since Indian legislation does not currently specify any particular registration or notification requirements for data processors or controllers, the law is correspondingly silent on the question of sanctions for failure to do the same.

The proposed Privacy Bill, 2011 includes, within the functions of the Data Protection Authority of India, the function of receiving and investigating alleged violations of data protection, as well as any data security breaches, and issuing appropriate orders as may be required to safeguard security interests of the data subjects in question.

The proposed Bill does state in Chapter X, section 60, that the penalty for failure to register will be a fine extending up to INR 500,000.

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

Neither the current nor proposed legislation prescribe registration fees.

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

Neither the current nor proposed legislation prescribe guidelines with respect to renewals.

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

The IT Act and associated amendments and rules do not prescribe prior approval requirements specifically with respect to data protection regulators. However, data controllers must obtain the consent of the data subject regarding the purpose of use before collecting any sensitive personal information. They must not collect any sensitive personal information unless:

1. the information is collected for a lawful purpose and is connected with a function or activity of the data controller; and
2. the collection of the information is considered necessary for that purpose.

The legislation – both current and proposed – does not address requirements for any other approval that data controllers are required to take, or what activities warrant said approval.

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

This is not applicable. See question 6.9 above.

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

This is not applicable. See question 6.9 above.

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

This is not applicable. See question 6.9 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.**

Neither the IT Act nor the IT Rules mention the appointment or role of a Data Protection Officer.

According to section 46 of the IT Act, an Adjudicating Officer shall be appointed by order of the Central Government for the purpose of discerning whether or not any person has contravened any provision of the IT Act. The Adjudicating Officer has the trappings of a civil court.

In addition, section 48 of the Act provides for the establishment – by notification – of an appellate tribunal known as the Cyber Regulations Appellate Tribunal. The tribunal will have an appellate jurisdiction and is entitled to exercise its jurisdiction both on fact and law over a decision or order passed by the Adjudicating Officer or the Controller of Certifying Authorities.

The appointments of both the Adjudicating Officer, as well as the Cyber Regulations Appellate Tribunal, are optional and entirely at the discretion of the Central Government. The Act does not specify which circumstances justify the appointment of the Adjudicating Officer or the Appellate Tribunal. It is also unclear whether such appointment is made *suo motu* or on representation by another party.

The proposed Data Privacy Bill, 2017 seeks the appointment of a Data Protection Officer having adequate technical expertise in the field of data collection or processing and the ability to address any requests, clarifications or complaints made with regard to the provisions of this Act, provided that the data controllers and processors employing less than 500 people and having a per capita turnover of less than one crore rupees may jointly appoint a Data Protection Officer, for resolving or addressing any requests, clarifications or complaints made herein in collaboration with other bodies with similar size or turnover.

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

The proposed Data Privacy Bill, 2017 provides that a complainant may approach the Data Privacy Authority for redressal of complaints.

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

The proposed Data Privacy Bill, 2017 provides that a complainant may approach the Data Privacy Authority for redressal of complaints.

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

Yes. See question 7.1 above.

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

Since the law does not address the appointment of a Data Protection Officer specifically, there are no statutorily prescribed qualifications for this position.

However, under section 46 of the IT Act, the Adjudicating Officer must not be below the rank of a Director to the Government of India, or an equivalent officer of the State Government, and must possess such experience in the field of information technology and legal or judicial experience as may be prescribed by the Central Government. If more than one Adjudicating Officer is appointed, the Central Government will determine the jurisdictional powers of the officers.

Under section 48 of the IT Act, the Central Government has been given a mandate to employ more than one Cyber Regulations Appellate Tribunal, but the language of Rule 13 of the Cyber Regulations Tribunal (Procedure) Rules (2000) makes it clear that there shall be only one tribunal. The tribunal must consist of one person only, referred to in section 49 of the Act as the Presiding Officer of the Cyber Appellate Tribunal. The qualifications of the Presiding Officer must be the following:

1. that he is, or has been, or is qualified to be, a Judge of the High Court; or
2. he is, or has been a member of the Indian Legal Service and is holding or has held a post in Grade 1 of that service for at least three years.

The Central Government has not so far appointed a Presiding Officer for the Cyber Regulations Appellate Tribunal.

See also question 7.1 above.

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

Section 46 of the IT Act mandates that an Adjudicating Officer is appointed by the Central Government for the purposes of holding an inquiry in the manner prescribed by the Central Government.

This section further states that the Adjudicating Officer shall, after giving the person who has committed the alleged contravention a reasonable opportunity for making representation in the matter, and if, on such inquiry, he is satisfied that the person has committed the contravention, may impose such penalty or award such compensation as he thinks fit in accordance with the provisions of that section.

Section 47 of the Act states that the factors to be taken into account by the Adjudicating Officer in determining the quantum of compensation are the following:

- (a) the amount of gain of unfair advantage, wherever quantifiable, made as a result of the default; and
- (b) the amount of loss caused to any person as a result of the default and the repetitive nature of the default.

The Cyber Regulations Appellate Tribunal, being an appellate body, has the power to examine the correctness, legality or propriety of the decision or order passed by the Controller of Certifying Authorities or the Adjudicating Officer under the IT Act. This power is absolute; which, by implication, bars the jurisdiction of civil courts to hear such appeals.

The Act grants an unconditional right of appeal to any aggrieved party to appeal an order made by the Controller or an Adjudicating Officer

under this Act. Further, the appeal before the Tribunal shall be filed within a period of 45 days from the date on which a copy of the order made by the Controller or the Adjudicating Officer is received by the person so aggrieved, according to section 57 of the Act.

The judicial function of the Cyber Regulations Appellate Tribunal is to give the parties to the appeal an opportunity to be heard, and to pass such orders thereon as it thinks fit, confirming, modifying or setting aside the order appealed against.

Under section 57, subsection 6 of the Act, the emphasis is on employing all 'judicial means' to dispose of the appeal within six months of the date of receipt of the appeal.

The Act further provides a second forum of appeal in the form of the High Court (the first being the Cyber Regulations Appellate Tribunal) to any person aggrieved by any decision or order of the Cyber Regulations Appellate Tribunal. An appeal is to be filed within 60 days from the date of communication of the decision or order of the Cyber Regulations Appellate Tribunal, on any question of fact or law arising out of said order.

In addition, the proposed Data Privacy Bill, 2017 states that the Data Protection Officer shall: (a) act as an independent person; (b) address requests, clarifications or complaints made in writing, including through electronic form, by any aggrieved person or legal representative thereof; (c) take steps to initiate an inquiry and commence proceedings within seven days of receiving the complaint; (d) resolve the matter within 90 days of receipt of the complaint; (e) recommend the data controller or processor to take action; and (f) record the proceedings, the results thereof and the reasons for arriving at the decision in writing.

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

Neither the IT Act and IT Rules nor the proposed Privacy Bills address the question of registration/notification of appointment of a Data Protection Officer 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?**

Neither the IT Act and IT Rules nor the proposed Privacy Bills address the question of naming the Data Protection Officer 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?**

Neither the IT Act and IT Rules nor the proposed Privacy Bills address this.

#### **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.)?**

Neither the IT Act and IT Rules nor the proposed Privacy Bills address this.

### **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 are no legislative guidelines or statutory regulations governing marketing communications through email or post. However, the Telecom Unsolicited Commercial Communications Regulations (2007) and the Telecom Commercial Communications Customer Preference Regulations (2010), both made under the Telecom Regulatory Authority of India (TRAI) 1997, regulate unsolicited commercial communications through telephone or by text. The Regulations state that telemarketers must register themselves with TRAI before they may send out marketing communication through telephone or text messages.

The Regulations also provide for those who wish not to receive unsolicited commercial communication to opt out of receiving said telephone calls or text messages. This is done simply by registering one's preference with the Customer Preference Registration Facility, which is statutorily required to be set up by the local access provider (defined in the Regulations as including the basic telephone service provider, the cellular mobile telephone service provider and the unified access service provider) or by registering with the National Do Not Call Register.

The proposed Privacy Bill, 2011, in Chapter VI, section 30, places restrictions on direct marketing. When the Bill is enacted, no person shall be permitted to hold or process a personal database used for direct marketing services, unless he is registered with the National Data Registry and one of the purposes of registration is in fact direct marketing, he has a record stating the source from which he obtained the personal data, and all the individuals whose data are contained in the database have consented to receive direct marketing communication from the person in question.

#### **9.2 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 question 9.1 above.

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

Neither the IT Act and IT Rules nor the proposed Privacy Bills address this.

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

Telemarketers may apply to Access Providers for telemarketing resources only after they have registered with TRAI. If telemarketers continue to send unsolicited commercial communication to telephone and mobile numbers who have registered themselves with the National Do Not Call Register or have opted out of receiving said communication with the Customer Preference Registration Facility, complaints may be made, toll-free, to the Access Provider, who then serves a notice upon the telemarketer in breach. Chapter III, Regulation



18 of the Telecom Commercial Communications Customer Preference Regulations (2010) provides for the blacklisting of telemarketers who have received said notice six times or more. No Access Provider is permitted to provide telecom resources to said telemarketer.

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

Neither current nor proposed legislation contains provisions on this matter.

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

See question 9.4 above.

### **10 Cookies**

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

Due to the fact that India has no comprehensive data protection regime, issues such as cookie consent have not so far been addressed by Indian legislation. It is planned that the Privacy Bill, 2011 will introduce data protection legislation more specifically targeted to issues of cyber security.

#### **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 above.

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

See question 9.4 above.

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

See question 9.4 above.

### **11 Restrictions on International Data Transfers**

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

Section 7 of the IT Rules states that bodies corporate can transfer sensitive personal data to any other body corporate or person within or outside India, provided that the transferee ensures the same level of data protection which the body corporate has maintained, as required by the IT Rules. A data transfer is only allowed if either:

1. it is required for the performance of a lawful contract between the data controller and the data subjects; or
2. the data subjects have consented to the transfer.

The proposed Privacy Bill, 2011, if enacted, will place slightly more stringent restrictions on international transfers of personal data. The Bill states in Chapter III, section 22 that cross-border transfers of personal data by data controllers shall not be permitted unless:

1. the transferee is subject to a law, code of conduct or contract which binds said transferee to principles of adapt protection substantially similar to those stipulated in the Privacy Bill;
2. the data subject consents to the transfer; or
3. the transfer is necessary in connection with a contract to which both the controller, as well as the subject, are parties.

#### **11.2 Please describe the mechanisms companies 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 a "Press Note" released on August 24, 2011, the Ministry of Information Technology clarified that the rules on sensitive data transfer described above are limited in jurisdiction to Indian bodies corporate and legal entities or persons, and do not apply to bodies corporate or legal entities abroad. As such, information technology industries and business process outsourcing companies ascribe to secure methods of data transfer which they prefer, provided that the transfer in question does not violate any law either in India or in the country to which the data is being transferred.

#### **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.**

Neither the current nor the proposed legislation specifies any requirements for registration or notifications for data transfers abroad. The requirements are limited to the criteria specified in question 11.1 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.)?**

The Whistle Blowers Protection Act, 2011 mandates that any public servant, or any person including any non-governmental organisation, may make a public interest disclosure before the Competent Authority. Section 4(6) of the Act states that no action shall be taken if the disclosure does not indicate the identity of the complainant. Section 6 mandates that the Competent Authority shall not take notice of any disclosure which relates to a matter or issue determined by a Court or Tribunal, to the extent that the disclosure seeks to reopen such matter or issue. It also mandates that the Competent Authority shall not investigate any disclosure involving an allegation if the complaint is made after the expiry of seven years from the date on which the action complained against is alleged to have taken place. Section 8 of the Act exempts matters related to the sovereignty, security and integrity of India, matters which may affect friendly relations with a foreign state, public order, decency or morality or in relation to contempt of court, defamation



or incitement to an offence pertaining to disclosure of proceedings of the Cabinet of the Union and State Government or any committee of the Cabinet from disclosure.

An amendment was proposed and passed by the Parliament to the Act. It seeks to further exempt: (a) information, the disclosure of which would cause a breach of parliamentary privilege; (b) information relating to commercial confidence, trade secrets or intellectual property, the disclosure of which would harm the competitive position of a third party, unless such information has been disclosed to the complainant under the Right to Information Act; (c) information which is available to a person in his fiduciary capacity; (d) information received in confidence from a foreign government; (e) information, disclosure of which would endanger the life or physical safety of a person or identify the source of information; and (f) information which would impede the process of investigation or apprehension or prosecution of offenders from disclosure. The amendment is yet to receive the assent of the President and be promulgated into law.

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

See the answer to question 12.1 above. There have been no reported instances where companies have had to address the issue of anonymous reporting.

## **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)?**

Current legislation does not touch upon questions relating to CCTV surveillance. However, the proposed Privacy Bill, 2011 states in Chapter V, section 26 that the installation and operation of CCTV surveillance in public areas shall be in accordance with prescribed procedure for legitimate and proportionate objectives, and will not affect his right to privacy. There are no registration requirements specifically laid out in this proposed legislation, neither does it elaborate on what the prescribed procedure for the installation and operation of CCTV will be.

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

Current legislation does not touch upon questions relating to CCTV surveillance. However, the proposed Data Privacy Bill, 2017 provides that, apart from reasonable restrictions such as safeguarding national security or defence of India, prevention of acts of terrorism, corruption, money laundering, organised crime, sale or purchase of narcotic and psychotropic substances, investigation of cognisable offences and maintenance of public order, no person shall conduct or assist in conducting any surveillance. Targeted profiling of individuals or of a certain section or class of persons without any basis is expressly barred. The onus to prove that information or personal data obtained through surveillance was so done while maintaining a proper chain of custody without any tampering or external interference, in a court of law, shall be on the concerned state authority, intelligence or private entity, as the case may be.

## **14 Employee Monitoring**

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

Neither current nor proposed legislation contains specific provisions relating to CCTV surveillance of employees. However, the proposed Privacy Bill, 2011, when in force, will ban covert, intrusive or directed surveillance except in certain specified circumstances, including objectives of national security or public safety. The proposed Bill also states that the provisions it contains relating to the storage, processing, retention, sharing, security and disclosure of personal data apply equally to data collected through surveillance. See also question 13.2 above.

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

Current legislation contains no provisions relating to requirements of consent from employees. However, the proposed Privacy Bill, 2011 bans covert surveillance, which suggests that consent will have to be obtained from employees once this law comes into force, although the Bill is silent on details relating to what qualifies as consent and how it may be obtained.

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

Neither current nor proposed legislation contains provisions on this matter.

## **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.)?**

Rule 8 of the IT Rules describes reasonable security practices and procedures as follows:

- 1) A body corporate, or a person on its behalf, shall be considered to have complied with reasonable security practices and procedures if they have implemented such security practices and standards, have a comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected and with the nature of the business in question.
- 2) In the event of an information security breach, the body corporate or a person on its behalf shall be required to demonstrate, as and when called upon to do so by the agency mandated under the law, that they have implemented security control measures as per their documented information security programme and information security policies. The international standard IS/ISO/IEC 27001 on "Information Technology – Security Techniques – Information Security Management System – Requirements" is one such standard.
- 3) Any industry association or an entity whose members are self-regulating by following codes other than the IS/ISO/IEC codes of best practice for data protection as per (1) above, shall get its codes of best practice duly approved and notified by the Central

Government. The body corporate or a person on its behalf, that has implemented either the IS/ISO/IEC 27001 standard or the codes of best practice for data protection as approved and notified under point (3) above, shall be deemed to have complied with reasonable security practices and procedures, provided that such a standard or such codes of best practice are certified or audited on a regular basis by an independent auditor, duly approved by the Central Government. This audit shall be carried out by an auditor at least once a year, or as and when the body corporate undertakes a significant upgrade of its process and computer resources.

In August 2011, the Ministry of Communications and Information issued a "Press Note" (*Clarification on the Privacy Rules*) which provides that any Indian outsourcing service provider/organisation providing services relating to collection, storage, dealing or handling of sensitive personal information or personal information under contractual obligations with a legal entity located within or outside India is not subject to collection and disclosure of information requirements, or consent requirement as detailed by the IT Rules, provided it does not have direct contact with the data subjects when providing their services.

The proposed Privacy Bill, 2011, which will override the IT Rules if enacted, also contains provisions pertaining to the security of personal data, stating specifically that every data controller must set appropriate technological, organisational and physical standards for the security of data under its control. In Chapter III, section 15 of the proposed Bill, it is also stated that the Data Protection Authority (the establishment of which is provided for in the same Bill) may prescribe regulations or codes of practice, laying down standards for technological, organisational and physical measures for protection of personal data, and that different standards may be prescribed for different classes of organisation.

**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) expects voluntary breach reporting.**

The current legislation contains no legal requirements to report data security breaches to either authorities or data subjects.

The proposed Privacy Bill, 2011, in Chapter III, section 16, prescribes that where a data controller has reasonable grounds to believe that the personal data of any data subject under its control has been accessed or acquired by unauthorised persons, the data controller must, as soon as is reasonably possible after discovering the breach, notify both the data subject and the Data Protection Authority. The notification shall be in writing, and shall be sent either to the last known address of the data subject by registered post requesting due acknowledgment, or published in at least two national newspapers. The notification must contain sufficient information as is necessary to enable the data subject to take steps to mitigate the potential consequences of the data security breach, including, if possible, the identity of the person who may have committed the breach and the date on which it occurred.

The proposed Data Privacy Bill, 2017 also mandates that every person shall have the right to be duly and promptly informed, within seven days, about any unauthorised access, destruction, use, processing, storage, modification, de-anonymisation, unauthorised disclosure (either accidental or incidental) or other reasonably foreseeable risks or data security breaches pertaining to their personal data.

**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) expects voluntary breach reporting.**

The current legislation does not contain any such requirement. However, as explained in question 15.2 above, the proposed legislation does. The only exception to the requirement in the proposed Privacy Bill that the data controller notify the data subject in the event of a breach is if the Data Protection Authority believes that such a notification will impede a criminal investigation, or if the identity of the data subject cannot possibly be identified.

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

As previously explained, the legislation currently in force does not deal with data breaches at all, except as indicated in question 15.1 above. The proposed Privacy Bill, 2011 elaborates on penalties for different types of breaches including violation of security/secretcy/confidentiality licences, unauthorised interception of communication (and disclosure of said intercepted communication), obtaining personal information on false premises, disclosure, data theft and contravention of the directions of the proposed Data Protection Authority. The penalties imposed are in the form of heavy fines, which vary for each offence but which do not extend beyond INR 1,000,000. The only exception to this is a penalty imposed for contravention of direction of the Data Protection Authority, which may extend to INR 200,000 and, in the case of a continuing breach, an additional sum which may extend to INR 200,000 for every day that the default continues.

## 16 Enforcement and Sanctions

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

Indian legislation does not specifically provide for the establishment and function of Data Protection Authorities, although proposed legislations seek to alter this.

**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?**

Indian legislation does not specifically provide for the establishment and function of Data Protection Authorities, although proposed legislations seek to alter this.

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

Indian legislation does not specifically provide for the establishment and function of Data Protection Authorities, although proposed legislations seek to alter this.

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

Indian legislation does not specifically provide for the establishment and function of Data Protection Authorities, although proposed legislations seek to alter this.

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

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

As long as requests from foreign companies are based on an order from a court of law and if the country in question has a reciprocal arrangement with India, then such a request may be enforced in India, if necessary, through an Indian court. Absent a court order, Indian companies do not have any obligation to respond to foreign e-discovery requests or requests for disclosure.

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

None. Please refer to section 16 above.

### 18 Trends and Developments

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

The Supreme Court of India, in the matter of *Justice K S Puttaswamy (Retd.) & Anr. versus Union of India & Ors.*, was posed with the question of whether or not privacy is a fundamental right guaranteed under the constitution at all.

The court ruled on the said question in affirmative and while doing so, observed that it is not an absolute right but subject to certain reasonable restrictions. On the aspect of data protection, the Court observed that the right of an individual to exercise control over his personal data and to be able to control his/her own life would also encompass his right to control his existence on the internet.

The judgment also details that consent obtained from users has to be informed consent given in an informed manner by users and cannot be shrouded in lengthy terms of agreements. The Court even upheld the right of an individual to be forgotten from the internet by observing that:

*“If we were to recognize a similar right, it would only mean that an individual who is no longer desirous of his personal data to be processed or stored, should be able to remove it from the system where the personal data/ information is no longer necessary, relevant, or is incorrect and serves no legitimate interest. Such a right cannot be exercised where the information/ data is necessary, for exercising the right of freedom of expression and information, for compliance with legal obligations, for the performance of a task carried out in public interest, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims. Such justifications would be valid in all cases of breach of privacy, including breaches of data privacy.”*

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

Following the Supreme Court Judgment in *Puttaswamy*, the Government set up an expert committee for a data protection framework in India under former Supreme Court Judge, B.N Srikrishna in August 2017. The committee was tasked with identifying key data protection issues in India and recommending methods of addressing them. The committee released a White Paper in November 2017, suggesting that a framework to protect data in the country should be based on seven principles: (i) the law should be flexible to take into account changing technologies; (ii) law must apply to both Government and private sector entities; (iii) consent should be genuine, informed and meaningful; (iv) processing of data should be minimal and only for the purpose for which it is sought; (v) entities controlling the data should be accountable for any data processing; (vi) enforcement of the data protection framework should be by a high-powered statutory authority; and (vii) penalties should be adequate to discourage any wrongful acts.

While the Government is yet to promulgate a law based on the committee’s report or pass a legislation, deliberations are ongoing.

**Hari Subramaniam**

Subramaniam & Associates (SNA)  
M3M Cosmopolitan, 7<sup>th</sup> Floor  
Sector 66, Golf Course Extension Road  
Gurugram – 122001  
National Capital Region  
India

Tel: +91 124 484 9700  
Email: [sna@sna-ip.com](mailto:sna@sna-ip.com)  
URL: [www.sna-ip.com](http://www.sna-ip.com)

Hari Subramaniam is an attorney-at-law with a background in medical sciences. He is the Managing Partner of one of the leading New Delhi-based law firms specialised in intellectual property rights (IPR), Subramaniam & Associates (SNA). He has been in practice in the field of patents and trademarks for 35 years and has been involved in several important IPR and contentious cases in India and abroad. He has one of the best track records in Patent Oppositions in India. He is a major contributor to, and speaker at: various workshops on intellectual property laws conducted worldwide, including: the World Intellectual Property Organization; leading universities around the world; the Intellectual Property Owners' Association, USA; the American Bar Association; Judicial Academies; the Indo-Pacific Juristic Forum; the International Association for the Protection of Intellectual Property; the Asian Patent Attorneys Association; the American Intellectual Property Law Association; and various Patent Offices. Mr. Subramaniam has authored several articles on patents and is on the teaching faculties of several institutions, such as: the Indian Law Institute, New Delhi; the Faculty of Law, New Delhi; and the Academy of Intellectual Property Laws, Mumbai. He has been invited several times as an expert witness before the Parliament for the amendment of patent laws. He was a member of the three-member team invited by the Mauritius Research Council, headed by the Prime Minister of Mauritius, to advise it on Patent Law amendments in August 2002. He has been recognised as a top-tier attorney by *IAMS, Managing Intellectual Property, The Legal 500 Asia Pacific, Asia Law*, etc., and has also won the "Leading IP Lawyer of the Year" award several times. He is a member of several international organisations connected with Intellectual Property and is the President of the Asian Patents Attorneys Association, India Chapter. He featured in *Asia Law's* "50 Leading IP Lawyers one must know in Asia and Asia Pacific".

**Aditi Subramaniam**

Subramaniam & Associates (SNA)  
M3M Cosmopolitan, 7<sup>th</sup> Floor  
Sector 66, Golf Course Extension Road  
Gurugram – 122001  
National Capital Region  
India

Tel: +91 124 484 9700  
Email: [asm@sna-ip.com](mailto:asm@sna-ip.com)  
URL: [www.sna-ip.com](http://www.sna-ip.com)

Aditi Subramaniam has a Bachelor's degree in English Literature from the University of Delhi and a Bachelor's degree in Law from the University of Oxford. She also holds a Master's Degree in Law (LL.M.), from Columbia University, New York, USA. She specialises in patent and trademark prosecution and contentious matters, including oppositions and appeals before the Intellectual Property Office and the Appellate Board, as well as litigation before the District and High Courts. She also advises clients on data protection, pharmaceutical advertising and cyber security. She is widely published and very well regarded in the Indian and international legal fraternity.



Subramaniam & Associates (SNA) – formerly Subramaniam, Nataraj & Associates – is a full-service IP firm with 20 highly qualified attorneys. It boasts a very impressive list of clients and represents several Fortune 500 companies, leading corporations, universities and law firms from all over the world. It also represents a large number of domestic corporations worldwide. The firm is equipped to provide complete and highly cost-effective services, from drafting, filing and prosecution of applications to searches, oppositions and enforcement. It has an excellent network of associates and correspondent counsels worldwide. SNA is one of the largest filers of PCT International Applications from India and is regarded by the Indian Patent Office and the industry as a top IP firm in India.

SNA provides its clients with a personalised service – professional in approach and reliable irrespective of any time constraints. It possesses the latest technology and sophisticated software to enable its attorneys to keep track of all critical deadlines. The work systems are adapted to meet the specific needs of each client.

SNA's team of attorneys includes specialists in different technical fields as well as in litigation. SNA's clients are assured of easy access to appropriate advice at different stages in the creation, filing, prosecution, protection, management, exploitation and enforcement of their intellectual property.

With representation in major cities of India, such as Calcutta, Chennai and Mumbai, and long-established relationships with local counsel throughout the world, SNA is well-positioned to serve its clients' domestic and international needs.



# Isle of Man

DQ Advocates Limited

Sinead O'Connor



Hazel Dawson



## 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 2002 (the “DPA”). The DPA came into operation on 1 April 2003 and is based upon the UK’s Data Protection Act 1998. The DPA gives effect within the Isle of Man to requirements equivalent to the European Directive 95/46/EC (“Directive”). From 25 May 2018, the DPA is intended to be replaced by the Data Protection Bill 2018 which will be 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 (“Orders”). The Bill, Regulations and Orders are all subject to consultation at the time of writing.

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

In addition to current Codes of Practice, the Regulations anticipate that the Information Commissioner will issue a data sharing Code, a direct marketing Code and any other Codes required to be issued by the Council of Ministers.

### 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.

Certain subordinate legislation modifies the right to subject access requests, generally in circumstances where compliance with a request would be likely to cause serious harm to the physical health, mental health or condition of the individual concerned. Such subordinate legislation includes:

- Data Protection (Subject Access Modification (Health) Order 2003 (SD 19/03));
- Data Protection (Subject Access Modification (Social Work) Order 2003 (SD 20/03)); and
- Data Protection (Subject Access Modification (Education) Order 2003 (SD 21/03)).

Data Protection (Subject Access Exemptions) (Adoption Etc.) Order 2003 (SD 22/03) exempts records and reports relating to adoption or parental orders from the data subject’s right of access under the DPA.

Data Protection (Corporate Finance Exemption) Order 2003 (SD 23/03) exempts from the data subject’s right of access data which if disclosed may affect the orderly functioning of financial markets or the efficient allocation of capital within the economy.

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

The IC is the independent supervisory body for data protection. The IC is also the supervisory body for the current Unsolicited Communications Regulations from 2005 (“UCR”), holds certain responsibilities in respect of the Isle of Man Government’s Code of Practice on Access to Government Information and 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 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. 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 which 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.

■ **“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, which allows or confirms 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, which reveals information about his or her health status.

■ **“Genetic data”** means personal data relating to the inherited or acquired genetic characteristics of an individual which gives unique information about the physiology or the health of that individual and which results, 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 controller is established in the Island and the personal data is processed in the context of the activities of that establishment.
- A data processor processing personal data where the processor is established in the Island and the personal data is processed in the context of the activities of that establishment.
- A data controller established outside the Island where the personal data being processed relates 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 relates 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 interest 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 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.

## ■ Other key principles – please specify

### ■ 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 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 Information Commissioner, if the data subjects lives 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 Information Commissioner.

### 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 broad description of the personal data being or to be processed and of the category or categories of the data subject to which they relate are sufficient. A broad description of the purpose or purposes

for which the data are being or are to be processed is also required as is a description of any recipient or recipients to whom the data controller intends or may wish to disclose the data. Finally, the names, or a description, of any countries or territories outside the Island to which the data controller directly or indirectly transfers, or intends to or may wish directly or indirectly to transfer, the data is needed for registration purposes.

**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 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 requirement to register applies to Isle of Man data controllers as well as foreign data controllers who have a nominated representative on the Island.

**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)?**

In addition to the information set out in question 6.2 above, the information which must be included in the registration is (a) the data controller's name and address, and (b) the name and address of any nominated representative.

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

Information about the sanctions for failure to register/notify under the revised law is not currently available. Under current law, any data controller who processes personal data without registering is guilty of an offence and is liable on summary conviction to a fine not exceeding £5,000.

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

The fee for registration under the revised law is not currently available. Under current law, the notification fee payable is £70.

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

It is anticipated that Notification Regulations will be introduced, which will require an annual renewal.

**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?**

There is no current facility for registration to be completed online.

**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 Information Commissioner's website.

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

Completion of the registration documentation is a relatively quick process and confirmation from the Information Commissioner is usually received promptly.

## 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 a penalty.

**7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect to 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. Local law will reflect the requirements of the GDPR which 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. As a matter of good practice, the WP29 recommends 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 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?)**

Under current law, the following provisions apply:

- Direct marketing activities must generally comply with the DPA 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 (SMS, email 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.

Under the proposed revised law, the Information Commissioner 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.

#### **9.2 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.)**

Under current law, the following provisions apply:

- Direct marketing activities must generally comply with the DPA 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 DPA.
- Persons marketing by way of live telephone calls may not make unsolicited calls if the individual or corporation contacted has either: (i) previously notified the person marketing that such calls should not be made to such individuals or corporations telephone number; or (ii) where 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) ("TPS").



- Automated telephone marketing calls may only be made with the consent of the individual or corporation to whom such calls are directed.

Under the proposed revised law, the Information Commissioner will issue a direct marketing Code containing practical guidance in relation to the carrying out of direct marketing in accordance with the requirements of the data protection legislation.

### 9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

The restrictions would only apply to marketing sent from the Island.

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

The current law provides the IC with no audit powers and no powers to issue fines to companies who breach marketing restrictions.

### 9.5 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.

### 9.6 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) ("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 ability for the IC to take 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 proposed revised law, 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 Information Commissioner in respect of any measures which the data controller is proposing to take in accordance with Recital 108 of the 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.

### 11.2 Please describe the mechanisms companies 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 Information Commissioner, when transferring personal data to a third country, 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.

Transfer of personal data to the US is also possible if the data importer has signed up to the EU-US Privacy Shield Framework, which was designed by the US Department of Commerce and the EU Commission to provide businesses in the EU and the US with a mechanism to comply with data protection requirements when transferring personal data from the EU to the US.

**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.**

Registration with the IC requires that the data controller specifies the names, or description of, any countries or territories outside of the Isle of Man to which the data controller may directly or indirectly transfer personal data. Notification is sufficient and no approval is required.

The proposed revised law requires approval from the Information Commissioner for any transfer of personal data to a third country which is not subject to an adequacy decision.

## 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 current or proposed revised law. 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, or strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do companies typically address this issue?**

There is no reference to whistle-blowing within the current or proposed revised law 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 IC to use CCTV. A separate notification is also not required. The use of CCTV must, however, be included in an organisation's data protection registration unless the organisation is in some way exempt. The Information Commissioner's guidance recommends the use of clear and visible signage which includes who to contact about the operation of the CCTV system. There is nothing in the proposed revised law which would appear to amend the current requirements.

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

The Information Commissioner's guidance states that there must be a lawful reason for considering the use of CCTV which cannot be met in another way. The Information Commissioner 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 which is undertaken and the reasons for it unless 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 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 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 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) expects 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) expects 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 which are other than those prescribed in the GDPR.

## 16 Enforcement and Sanctions

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

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
Information Notice – requires a controller or processor to provide the Information Commissioner with the information that he reasonably requires.	On summary conviction, a fine not exceeding £5,000 or to custody of not more than six months or both. On conviction on information, an unlimited fine.	-
Assessment Notice – requires a controller or processor to permit the Information Commissioner to carry out an assessment of compliance with the data protection requirements.	As per any Penalty Notice issued by the Information Commissioner.	-
Enforcement Notice – requires the recipient to take the steps specified in the Notice or refrain from taking the steps specified in the Notice.	As per any Penalty Notice issued by the Information Commissioner.	-
Powers of entry and inspection.	Various penalties in relation to obstructing or failing to assist.	-

**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 proposed revised law would entitle the Information Commissioner 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 companies established in other jurisdictions? If so, how is this enforced?**

Enforcement to date has been limited to Enforcement Notices and Formal Undertakings against Isle of Man data controllers.

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

### 17.1 How do companies 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.

The IC's website lists four Enforcement Notices served from 2012 to date. These relate to (i) the processing of personal data from surveillance equipment on buses without the appropriate signage, (ii) the sending of direct marketing by email without proper regard for data protection and other regulatory requirements, (iii) matters connected to (i), and (iv) proper compliance with the right of data subject access. Two formal undertakings have also been issued in 2017 relating to a data subject access request and the improper publication of personal data. The issue of these undertakings is indicative of increased enforcement activity by the IC.

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

The Information Commissioner is very much focused on the proposed revised law to implement the GDPR as well as in trying to publish guidance and resources to assist data controllers and processors to comply.



**Sinead O'Connor**

DQ Advocates Limited  
The Chambers, 5 Mount Pleasant  
Douglas, IM1 2PU  
Isle of Man

Tel: +44 1624 626999

Email: [sinead@dq.im](mailto:sinead@dq.im)

URL: [www.dq.im](http://www.dq.im)

Sinead O'Connor is DQ's Head of Regulatory & Compliance Services and is a member of the Data Protection Team. Sinead advises clients on the regulatory and compliance aspects of data protection and the GDPR, in particular on the implications of the GDPR for data retention and on the general impact on data protection policies. 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.

**Hazel Dawson**

DQ Advocates Limited  
The Chambers, 5 Mount Pleasant  
Douglas, IM1 2PU  
Isle of Man

Tel: +44 1624 626999

Email: [hazel.dawson@dq.im](mailto:hazel.dawson@dq.im)

URL: [www.dq.im](http://www.dq.im)

Hazel Dawson is a senior associate in DQ's Corporate and Commercial department and is a member of the Data Protection team. Hazel, who is a qualified data protection practitioner, has experience of advising a wide-ranging client base on the provisions and requirements of the current data protection legislation together with advising on the preparations necessary for compliance with the GDPR. As part of her varied practice, Hazel has experience in advising Isle of Man-based e-business and technology companies in relation to general corporate matters, website terms and privacy notices and the outsourcing of obligations to third-party service providers.



DQ Advocates is a leading Isle of Man-based law firm with an international reach.

We offer a full range of legal, regulatory and compliance services to our local and global clients.

DQ are accessible, responsive and commercial with client-oriented strategies and goals. Our specialist lawyers are recommended as leading lawyers in *Chambers & Partners* and *The Legal 500*.

# Israel

Dalit Ben-Israel



Naschitz, Brandes, Amir & Co., Advocates

Efrat Artzi



## 1 Relevant Legislation and Competent Authorities

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

The Protection of Privacy Law, 5741-1981 (“**PPL**”), and Regulations promulgated pursuant thereto (especially the Privacy Protection (Data Security) Regulations, 5777-2017, effective as of May 2018 (“**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**”).

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

The Credit Data Law, 5776-2016 (“**Credit Data Law**”), and Regulations and Rules enacted therefrom govern data protection in a new system 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 Regulations promulgated therefrom; and there are specific sectors which are subject to additional regulatory requirements.

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

The Database Registrar (“**Registrar**”) forms 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 personal information held in digital databases (“**PPA**”). The Registrar issues formal guidelines on privacy and data protection which apply to all sectors. Recently, PPA issued guideline 3/2018 (“**ISO Guideline**”), according to which, organisations which are certified by the ISO/IEC 27001:2013(E) standard and fully comply with its terms will be considered as complying with the Security Regulations (as long as they have a valid certification), and provided that they comply with specific requirements under the Security Regulations, as detailed in the ISO Guideline.

The Israel National Cyber Authority (which forms part of the Prime Minister’s office) is responsible for protecting civilian cyber space.

The Supervisor of Credit Data Sharing 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, personal status, intimate affairs, state of health, economic position, vocational qualifications, opinions and beliefs of an individual (defined as “**Information**”).
- **“Processing”**  
Includes disclosure, transfer and delivery (defined as “**Use**”).
- **“Controller”**  
Whoever is responsible for all aspects associated with Databases (no formal definition, referred to as the “**Database Owner**” or “**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.
- **“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 Constitutional, Law and Justice Committee of the Knesset’s approval, as being sensitive Information (defined as “**Sensitive Information**”).
- **“Data Breach”**  
Any incident which raises a concern to: the integrity of the Information; unauthorised use of the Information; or use without lawful permission (defined as “**Data Breach Incidents**”).
- *Other key definitions – please specify (e.g., “Pseudonymous Data”, “Direct Personal Data”, “Indirect Personal Data”)*  
“**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; 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.

**“Direct Mailing Services”**: enabling others to engage in Direct Mailing by way of transferring lists, labels or data to others by any means.

**“Database Manager”**: active manager of an entity who Owns or Holds a Database, or a person who was authorised for this matter by such manager.

**“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 if the integrity of the Information was compromised; and (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 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?

PPL has no extraterritorial scope and only applies to Israel-based businesses.

### 4 Key Principles

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

- **Transparency**  
PPL (section 11) states that any request from a person to store or use his/her Information in a Database should be accompanied with a notice indicating: whether such Information is requested based on law or legal requirement, or on free will; the purposes for which the Information is requested; and who are the recipients of the Information, and for what purpose they will receive such Information.
- **Lawful basis for processing**  
PPL (section 8) states that managing or possessing a Database which requires registration with the Registrar must be registered. For processing activities, see “Transparency” above. Under the Registrar’s outsourcing services guidelines (2/2011), collection of data through illegal means or use of Information which was unlawfully obtained is prohibited.
- **Purpose limitation**  
PPL (section 8(b)) prohibits the use of Information in a Database for any purpose other than for which the Database was established. Use/transfer to others of Information about an individual’s private affairs for another purpose, without the individual’s consent, constitutes a breach of privacy (section 2(9) of PPL). Similar provisions appear in the Credit Law.
- **Data minimisation**  
The Owner is required to annually check whether the Information in its Databases is not over the amount required for the purposes it was collected for.
- **Proportionality**  
The Basic Law (section 7) defines privacy as a constitutional

right, and case law extended it to data protection (see the *Isakov* case). The proportionality principle was introduced through the Basic Law (section 8), and was also adopted in the Registrar’s guidelines (4/2012 and 5/2017) on CCTV cameras (in public places and workplaces), stating, generally, that the use of surveillance means should be proportionate, transparent, reasonable and fair.

#### ■ Retention

PPL does not refer to data retention, but section 14(a) allows Data Subjects to ask for the deletion of their Information.

Security Regulations require outsourcing service agreements to include the Holder’s obligation to delete Information following the completion of the services; the Registrar emphasises in guideline 2/2011 that deletion applies to all media (including backup), and should be accompanied by the Holder’s affidavit, confirming such obligation. To the extent access is required for claim defence purposes, data will be retained with a third-party escrow.

The Credit Law includes specific retention periods for the credit data in the national repository.

According to the Registrar Recruiting Guideline (2/2012), employers and placement services must destroy or anonymise a candidate’s Information immediately upon the termination of using it (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).

#### ■ Other key principles – please specify

There are no other key principles to be aware of.

### 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**  
PPL (section 13(a)) entitles Data Subjects to inspect the Information about them in a Database. Case law extended this right to obtaining a copy of such Information. According to the Registrar’s guideline (1/2017), this right applies to data in any format or file type (including video, text messages and voice recordings). There are some exceptions, such as: physical or mental health Information; violation of legal privilege; investigations and law enforcement, etc. See also “CCTV” below.
- **Right to rectification of errors**  
PPL (section 14(a)) entitles a Data Subject to submit a request to the Owner (and if the Owner is a non-resident, to the Holder) to amend or delete any Information about him/her, if it is incorrect, incomplete, unclear or outdated. The Owner will inform the Data Subject whether it agrees to or refuses such request: Agreement (or if requested due to a court order) obligates the Holder to correct or delete the Information; and Refusal entitles the Data Subject to appeal to the competent court.
- **Right to deletion/right to be forgotten**  
For Deletion: see the previous section. The Data Subject is also entitled to be deleted from a Database used for Direct Mailing. The Registrar’s guideline (2/2017) expands such right to databases for Direct Mailing Services, and states that when the Database is being used for additional purposes, deletion is limited only to the Direct Mailing mailing list. The Biometric Law includes provisions for deletion (adults and minors under the age of 16).
- **Right to object to processing**  
PPL does not address this right specifically. As processing

requires the Data Subject's Consent or authorisation by law, the Data Subject can object to processing by withdrawing its consent or challenging the legal basis for processing. 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 the previous section.
- **Right to data portability**  
This is not applicable in our jurisdiction.
- **Right to withdraw consent**  
There is no specific provision, but it is implied from processing based on Consent. See "Marketing" below.
- **Right to object to marketing**  
See "Marketing" below.
- **Right to complain to the relevant data protection authority(ies)**  
PPL does not grant a Data Subject the right to complain to PPA, but rather to appeal or file a claim in a competent court. However, PPA handles Data Subjects' complaints as part of its enforcement and supervisory activities.
- **Other key rights – please specify**  
There are no other key rights to be aware of.

## 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 exemptions, the Database must be registered with the Registrar if it contains: Information on more than 10,000 Data Subjects; Sensitive Information; Information about Data Subjects, which was not provided by them, on their behalf or subject to their Consent; belongs to a public entity; and/or is used for Direct Mailing Services. Processing activities should be described in the registration form.

### 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 form must be filled in in its entirety, according to the questions and categories requested therein. All processing activities and all of the kinds of Information included in the Database should be detailed, and the Registrar may request additional details, explanation and clarifications.

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

For each 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)?

A registration obligation applies to the Owner. PPL does not specifically address applicability to Israeli citizens, residents or territoriality; however, case law implies that the registration obligation applies to Israeli Data Subjects, regardless 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 Owner's name, registration number and contact 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 it.

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

It is a criminal offence which is punished with one-year imprisonment and the imposition of administrative fines (up to 2,000 NIS for individuals and 10,000 NIS for corporations).

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

It is free of charge.

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

PPL (section 9(d)) requires that the registration form will be updated in case of changes in the information previously reported. 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?

No, but the Registrar's confirmation to the Database forms a pre-condition for its Use. PPL (sections 8 and 10(b1)) states that if a registration request is not responded to within 90 days following its submission, the Database can be used even though it has not been registered.

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

Yes, it can.



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

No. There is an online registry which allows searching for specific registrations by submitting queries (regarding the Owner's name, registration number, etc.), and receive partial information from the completed registration.

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

From a few days to 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.**

PPL (section 17B) requires the appointment of a security supervisor ("DPO") in the following circumstances: a Holder of five Databases that require registration; a public body as defined in PPL (section 23); a bank, insurance company, company involved in rating or evaluating credit. PPA recommends that the Owner and the Holder appoint a DPO when processing Information through outsourcing. The Biometric Law (section 26) mandates the appointment of a DPO for the biometric Database.

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

It is a criminal offence which is punished with one-year 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 to his or her role as a Data Protection Officer?**

No, but the DPO does not assume personal liability.

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

Yes, provided it does not constitute conflict of interests with his/her obligations as a DPO.

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

PPL (section 17B) requires that the DPO must be competent and qualified. A person convicted of an offence involving moral turpitude or of PPL provisions cannot be appointed. Security Regulations stipulate that the DPO shall report directly to the Database Manager or to an active manager of the Owner or the Holder, as the case may be, or to another manager who himself/herself directly reports to the Database Manager.

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

According to PPL (section 17), the DPO is responsible for the information security in the Databases. Security Regulations elaborate and add the following specific duties: preparation of a security procedure/policy and approving it with the Owner; and preparation and execution of a plan to control and oversee the compliance with the Security Regulations, and reporting its findings to the Owner and the Database Manager.

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

Yes, annually.

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

See the previous section.

**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 some circumstances (such as outsourcing services involving Information/Sensitive Information, and the banking and insurance sectors), the business and the Holder are required to enter into an 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.)?**

Security Requirements and the Registrar's guideline (2/2011) require the following (no specific format) to be addressed: the scope and kind of Information and systems the Holder is allowed to use, and the purpose(s) for such use (including permitted activities during such use); the Holder's obligation for deletion of the Information following termination of the agreement; security requirements; written confidentiality, data protection and use of Information for specific purpose by the Holder's representatives; compliance report with the Security Regulations (at least annually); and reporting 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?)**

PPL defines "Direct Mailing" as contacting a person on his/her belonging 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 executed in any media, and may have 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, PPA recommends indicating the circumstances under which it was provided, and allow the Data Subject to opt-out and incorporate 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.

The Communications Law (Telecommunications and Broadcasts), 5742-1982 ("Spam Law"), defines "Spam" as automated messages sent electronically (via email, SMS, fax or automatic dialing system) to an unknown recipient list, mainly for marketing and promotional purposes. Except for two exemptions, sending Spam requires the recipient's opt-in consent.

**9.2 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 will not be considered as Spam and there are no special requirements, unless the activity is considered "Direct Mailing".

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

No, they do not.

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

PPA enforces breaches of Direct Mailing and Direct Mailing Services; claims for sending Spam are not under PPA's authority.

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

Yes. PPA recommends the following: the Purchaser will receive the Seller's written confirmation that its activities are legal, and it fully complies with PPL requirements; the Seller duly registered a Database, lawfully collected the Information, and holds a list indicating the source from which the Information was acquired, and the identity of a 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 Consents for such purposes.

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

For sending Direct Mailing from a Database for Direct Mailing

provisions: administrative fines (up to 3,000 NIS for individuals and 15,000 NIS for corporations). For Spam: 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 is no reference to cookies under PPL and the Regulations. PPA recently issued recommendations for businesses operating websites/applications for online trading, which require the incorporation of a privacy policy, which, *inter alia*, explains what kind of information is being collected and for what purpose(s). PPA also requires the differentiation between information knowingly provided by the user and the information collected about the operation of the website/application (which may be collected by cookies).

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

No applicable restrictions, see previous question.

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

No, they have not.

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

This is not applicable in our jurisdiction.

## 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"), govern the transfer of Information from Databases abroad. The Transfer Regulations restrict the ability to transfer Information abroad, unless the law of the country to which the Information is transferred ensures a level of protection no lesser than under Israeli law. Transfer is also allowed when: 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 that commits contractually 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 or which receives data from Member States of the European Community, under the same terms of acceptance.

When transferring Information according to the above mechanisms, the Owner should ensure, in a written agreement with the recipient, 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 companies 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 is to use Regulation 2(8) of the Transfer Regulations, which allows the transfer to an EU country, or to receive the recipient's contractual obligation to comply with the requirements of Israeli 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.**

PPL (Section 9(b)(4)) requires notification in the registration form; however, this is no longer required in the registration form.

## 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 our jurisdiction.

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

No, it is not.

## 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. The Registrar's guideline (4/2012) on Surveillance Cameras in public areas ("CCTV Guideline"), in combination with section 11 of PPL, require notice in the form of clear, legible signs posted both at the entrance to the location of the cameras and in the area covered by the cameras. Notices should include an image, the name of the entity installing the cameras, the purpose (e.g., "theft prevention", "safety and security", etc.) and reference to where the full policy can be accessed (website) or contact details for further information. The full policy should include: the camera locations; the entity which installed the cameras; whether the images are recorded; the filming and recording purposes; the retention periods; the filming times; the entity responsible for viewing and storing the recordings; and the Database Manager and contact information for exercising the Data Subjects' rights.

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

The CCTV Guideline requires that the need for CCTV cameras and its impact on privacy will be evaluated against less invasive alternatives, and their use achieves a proper purpose. Privacy by Design is a consideration when deciding on the relevant parameters when installing CCTV cameras. Special care is required in certain circumstances, such as in public areas frequented by minors, facial recognition, where CCTV footage is matched with other Information in a Database, etc. Recording is allowed only if required to achieve the CCTV camera's purpose. Retention periods need to be defined. Data Subjects have inspection rights of footage only where the images enable Data Subject identification and provided recordings are retained for more than 30 days. Data inspection requests must be specific and should be evaluated with caution since other Data Subjects are likely to appear in the recordings.

## 14 Employee Monitoring

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

Employee monitoring by an employer will be construed narrowly, and may include any of the following.

The *Isakov* case (Labour Appeal 90/08 *Tali Isakov Inbar v. Commissioner for Women Labour*), rendered in 2011, imposed restrictions on monitoring employee emails and use of the workplace computer systems. The judgment differentiates between three types of email accounts: professional – intended only for work communications and which does not allow personal correspondence; external personal – employees' private email accounts; and dual use: for both personal and work purposes.

The professional account may be subject to monitoring, surveillance and backup. However, if an employee uses a professional account also for personal emails, the employer may access the personal communications only subject to the employee's explicit, informed and freely given consent, and only if the personal messages are unlawful or abusive. The external personal account may not be monitored except by a court order.

Personal messages in the dual account may be monitored only if: unusual circumstances that justify access to the messages; 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 Registrar's guideline (5/2017) regarding Workplace Surveillance ("Workplace Guidelines") emphasises the main principles applicable to surveillance means in workplaces. The installation of surveillance means is only allowed 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 will establish a clear and detailed policy regarding the manner and the extent of the usage, and its purposes, to be presented to the employees. The Workplace Guidelines include parameters regarding specific justifications required for the installation of surveillance means in certain sensitive areas.

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 the collecting and storing 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 will be enacted or by a freely given specific consent of the employee.

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

Consent is required for any breach of privacy under PPL; therefore, it is required when employee Information is collected, used or transferred other than for the explicit purpose of the employment. As opposed to the language of PPL which enables explicit consent, it has been determined by case law that due to the unbalanced employer-employee relationship, consent of an employee 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 approve reading them. According to the *Iskaov* case, the employer needs to have in place a policy for 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 a section or annex in 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. The employee needs to approve the policy in advance and to provide specific explicit, informed and freely given consent for each case of monitoring of the personal emails. The Workplace Guidelines require an 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. The Registrar Recruiting Guideline (2/2012) states that if, on or before the day on which a candidate was tested, he/she gives consent to any additional uses of the data collected in the recruiting process (that were not required for the purposes of completing the recruitment procedures of the specific employer), it shall be deemed as consent given without free choice and therefore invalid. The aforementioned consent of the candidate is only likely to be valid and based on real freedom of choice if it was given after receiving a notification regarding his acceptance or rejection for the position for which he was originally tested. The *Kalansua* case requires specific freely given consent for collecting and storing biometric data.

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

There are no statutory requirements. General case law requires consultation with unions when employee rights may be affected. Certain collective bargaining agreements, if applicable, may require notification or consultation in specific cases. The Workplace Guidelines require that the policy for use of CCTV in the workplace is defined, to the extent possible, after consultation with the employees' representatives.

## **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.)?**

PPL (section 7) defines Data Security as protection of the integrity of the Information or protection of the Information from being exposed, used or copied, without lawful permission. The Security Regulations elaborate details of security requirements, on a risk-based approach differentiating between four types of databases. Owners, Holders and Managers of Databases are each held individually responsible for data security according to PPL (section 17).

### **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) expects voluntary breach reporting.**

Security Regulations requires that Data Breach Incidents be documented, preferably by automated means, and discussed on a periodic basis depending on the Database's level of security. An Owner is required to report to the Registrar immediately (according to PPA, it means within 24 hours and no later than 72 hours as of the disclosure) of any Severe Data Breach Incident and the measures taken to mitigate it. Such report will be submitted online, based on a standard format which will be published on PPA's website. Following consultation with the national cybersecurity authority, the Registrar may instruct the Owner to notify the affected Data Subjects.

### **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) expects voluntary breach reporting.**

No legal requirements exist unless otherwise instructed by the Registrar.

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

Currently, there are none; see section 18. However, based on PPA's guideline (issued on May 2018), PPA set forth a transition period, during which PPA will gradually enforce its power regarding Severe Data Breach Incidents (see section 16 below).



## 16 Enforcement and Sanctions

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

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
Audits, criminal and administrative investigations.	Administrative fines upon individuals (2,000 NIS–5,000 NIS), and five-fold for corporations, for breach of PPL (section 31A), according to Administrative Offences Regulations (Administrative Fine – Protection of Privacy) 2004. For continuing violations, one-tenth of the fine for each day of the violation.  In addition, civil sanctions (including, without limitations, Severe Data Breach Incidents) may, <i>inter alia</i> , include: instructions for repair of security breach; determining a breach of PPL and/or Regulations; breach publication on PPA's website; and postponement or cancellation of a Database's registration, etc.	Criminal investigations. Findings will be provided to the Prosecutor to decide whether to start a criminal procedure.

### 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, when such activity is illegal (a court order is not required). See "Lawful basis for processing" and question 16.1 above.

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

PPA enforcement applies to all sectors, in order to reduce data risks.

On March 2018, PPA imposed administrative fines (100,000 NIS) on an Israeli company that used a software tool (which was based on a stolen database) enabling it to identify and approach individuals by using their stolen information and offer them services (including Direct Mailing not in accordance with PPL).

On February 2018, PPL completed a criminal investigation involving the illegal disclosure of Sensitive Information about women who intended to have an abortion to a non-profit organisation that tried to dissuade such women from having an abortion. PPA's findings were transferred to the Prosecutor to decide on further action.

On January 2018, PPA completed the investigation of a leakage of Data Subjects' Information or Sensitive Information to the internet. The company which provided IT services for the respective system was instructed to forthwith stop the leakage and conduct a comprehensive investigation. PPA concluded the IT service provider breached its obligations under PPA and the Regulations.

On May 2017, PPA imposed administrative fines (55,000 NIS) on an Israeli political party "Yesh Atid", a non-profit organisation and the head of such organisation, for several breaches of PPL, which resulted in a breach of privacy of Data Subjects stored in their Database.

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

PPA has no authority abroad, but regularly collaborates with and has an intensive dialogue with foreign data protection authorities.

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

### 17.1 How do companies 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, taking into account 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 component authority in the requesting country.

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

This is not applicable in our jurisdiction.

## 18 Trends and Developments

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

Enforcement through class actions, with a few pending actions.

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

On February 2018, a proposed amendment of PPL ("Bill") was published by the Israeli Parliament. The Bill proposes to enhance PPA's supervision and enforcement of PPL, particularly by authorising PPA to impose administrative fines. The Bill provides a scale of maximum fines on the basis of the volume of data processed, its sensitivity and the severity of the breach. The Bill will enable PPA to impose initial fines of 5,000 NIS (approx. 1,170 EUR) to 800,000 NIS (approx. 186,910 EUR). Severe violations can increase the fines two- or four-fold, meaning fines could reach 3,200,000 NIS (approx. 748,030 EUR). Fines cannot be reduced by PPA unless the circumstances for the reduction will be included in a list to be published by the Minister of Justice.

PPA intends to publish specific guidelines, such as in relation to operating drones.



**Dalit Ben-Israel**

Naschitz, Brandes, Amir & Co., Advocates  
5 Tuval Street  
Tel-Aviv 6789717  
Israel

Tel: +972 3 623 6010  
Email: [dbenisrael@nblaw.com](mailto:dbenisrael@nblaw.com)  
URL: [www.nblaw.com](http://www.nblaw.com)

Dalit is an expert in the fields of Computer, Information Technology, Cyber, Privacy and Data Protection Law and represents corporations in a broad range of international and domestic corporate and commercial transactions, with emphasis on information and technology transactions, including computer and communication transactions. Dalit is an expert in information technology transactions, including licensing, cloud and SaaS offerings, big data, open source, outsourcing and complex project agreements as well as internet-related legal and contractual issues. Dalit also has vast expertise in privacy including GDPR compliance, data protection, internet and application terms of use, privacy statements, internet domain disputes, drafting data security policies and procedures, spam issues, cybersecurity and regulatory consulting in these areas to diverse clients, *inter alia*, in the financial and insurance sector. Dalit is a member of the AIPPI – The International Association for the Protection of Intellectual Property and IAPP – The International Association of Privacy Professionals.

**Efrat Artzi**

Naschitz, Brandes, Amir & Co., Advocates  
5 Tuval Street  
Tel-Aviv 6789717  
Israel

Tel: +972 3 623 6050  
Email: [eartzi@nblaw.com](mailto:eartzi@nblaw.com)  
URL: [www.nblaw.com](http://www.nblaw.com)

Efrat specialises in the field of commercial law, and provides legal services in the fields of Data Protection and Privacy Law, Hi-Tech, Information Technology and Intellectual Property. During the course of her work, Efrat provides legal consultation to the firm's clients in diverse aspects of privacy law and data protection (under Israeli law and under the GDPR), has vast experience in drafting internet and applications terms of use, privacy policies and privacy notices, data protection policies and procedures, and has 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, in their ongoing activities. Efrat is a member of the IAPP – The International Association of Privacy Professionals.

נשיץ ברנדס אמיר  
NASCHITZ BRANDES AMIR

Naschitz Brandes Amir is one of Israel's largest and most prestigious full-service law firms, with an international and domestic practice that embraces the entire spectrum of civil matters. With over 160 legal professionals, the firm represents some of the world's largest companies in corporate, commercial and litigation matters, in Israel and abroad.

We provide comprehensive assistance and guidance to domestic and international clients on all aspects of privacy, data protection, cybersecurity and information law, including:

- assisting clients in the various stages of compliance and implementation of local regulations (such as the Privacy Protection Regulations (Data Security), 2017) and foreign regulations, currently mainly the EU General Data Protection Regulation;
- online marketing;
- cross-border data transfers;
- drafting and negotiating terms of use, privacy statements and notices, data security policies and procedures;
- spam issues;
- cybersecurity;
- data breach incidents and responses to enforcement authorities;
- domain name disputes; and
- cyber, spam and privacy related litigation.

# Italy

Julia Holden



Benedetta Marsicola



Trevisan & Cuonzo Avvocati

## 1 Relevant Legislation and Competent Authorities

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

From 25 May 2018, the principal data protection legislation in the EU will be Regulation (EU) 2016/679 (the “**General Data Protection Regulation**” or “**GDPR**”). The GDPR repeals Directive 95/46/EC (the “**Data Protection Directive**”) and leads 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?

Prior to the entry into force of GDPR, the main legislation on data protection was the so-called “Privacy Code”, Legislative Decree No 196/2003 of 30 June 2003 and further amendments. The Privacy Code will not be repealed “tout court” with the entry into force of the GDPR. The so-called “European delegation Law” No 163/2017 of last October 2017 assigned the Government with the task of adapting the national legislation to the upcoming EU rules within a six-month period. So far, the “European Law” No. 167/2018 and the last yearly Budget Act have introduced some specific rules. The current regulatory position Italy is therefore in a “work in progress” phase, and some aspects are still uncertain. This questionnaire has been filled based on the information and on the legislation currently in force at the date of submission.

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

Below there is a non-exhaustive list of legislation having an impact on data protection:

- the so-called “Statute of the Employees”, Legislative Decree No. 300/1970 basically provides for criminal sanctions against those employers who excessively control employees beyond what is necessary for working purposes (see section 14);
- Legislative Decree No. 81/2008 on safety and health at work; and
- Legislative Decree No. 206/2005, the so-called Consumer Code.

The Italian Data Protection Authority regularly issues sector-specific guidelines, such as:

- “Guidelines on the processing of data in the relationship between banks and their clients” of 25 October 2007 [doc. No. 1457247];
- “Guidelines on the health-related file” of 4 June 2015 [doc. No. 4084632]; and
- “Guidelines on the processing of personal data contained in administrative documents and documents processed by public entities for publication and dissemination on the web” of 2 March 2011 [1793203].

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

The authority responsible for data protection in Italy is the “Garante per la Protezione dei dati personali”, also called “Garante della Privacy”, established in 1996 with Law No.675/1996 (hereinafter referred to as the “Garante”). Among the many tasks of the Garante, there are: the monitoring of the compliance of the processing of data with the law; examining claims and reporting; banning illegitimate processing; issuing general authorisation orders; disseminating information of data protection; collaborating with the legislature for the drafting; and enforcement of the law.

## 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.

The Italian Privacy Code also contains the following additional definitions:

- **“Identifying data”** means the personal data allowing to directly identify a data subject.
- **“Judicial data”** means those data providing information on whether a data subject was investigated, charged and/or convicted for certain crimes.
- **“Anonymous data”** means those data which originally, or following processing, cannot be associated to any specific 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?

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 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 interest 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 was 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 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 Italian Data Protection Authority, if the data subjects lives in Italy or the alleged infringement occurred in Italy.

■ **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?

The Italian Privacy Code (Art. 37 and *ff.*) provides for the obligation to notify the Garante of the processing of certain types of data which could be particularly sensitive, such as genetic data, data indicating the geographic position of a person or object during a communication, data related to the sexual or psychic health of a person and data detained by specific types of entities, sensitive data stored for staff recruitment purposes, etc. The Garante is allowed to extend the list of the types of processing which need prior notification.

Also, the data controller should communicate in advance to the authority any processing of data capable of revealing the state of health of a data subject as a result of a health research programme or when the processing implies a transfer of data between public authorities (Art. 39 Italian Privacy Code).

The GDPR system is driven by a different general rule. Under the GDPR, the controller carries out a prior assessment of the risk connected with the data treatment and only where it determines there is a high risk, the controller must consult the authority prior to processing such data (Art. 36 Italian Privacy Code).

It still remains to be seen whether the Italian implementation of the GDPR will expressly repeal the obligation of prior notification under the Italian Privacy Code.

### 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 according to Art. 37 of the Italian Privacy Code should be carried out on one single occasion before the start of the data processing. It should include the personal data of the data subject(s), the purpose of the data processing activity and a general description thereof, in order to allow the Garante to assess the adequacy of the measures adopted with a view to ensuring the safety of the data processing.



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

Notification according to the Italian Privacy Code is carried out with respect to each data subject(s) based on the relevant data category and 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)?

Notifications according to the Italian Privacy Code are carried out by the data controller. The data controller is the entity or entities (local or foreign) having actual autonomous decision-making power over the purposes and methods of the processing in relation to the personal data they control, and should not be limited by choices made at the middle or top level of the 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)?

See question 6.2.

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

According to the Italian Privacy Code, failure to notify or communicate data processing according to Articles 37 and 39 is subject to an administrative sanction of EUR 20,000 to EUR 120,000.

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

There is administrative fee of EUR 150 per notification.

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

According to the Italian Privacy Code, the notification should be done only once before the start of the processing of data. However, the notification shall be renewed in the event that there are updates to the information contained in the initial notification.

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

The processing of sensitive data is conditional upon the prior approval by the Garante. However, the Garante regularly issues general authorisation for certain types of processing (such as for processing by freelance workers, processing by associations and foundations, processing for scientific research, etc.).

The processing of data different from sensitive data and judicial data, and which implies specific risks for the fundamental rights and for the dignity of the data subject, shall undergo a prior check by the Garante.

According to Art. 39 of the Italian Privacy Code, data processing can be started after 45 days from communication to the Garante in the absence of any response. However, the Garante can issue a later communication to the data controller ordering to cease the treatment or amend the manner thereof.

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

Yes, it has to be completed online on the Garante website according to the Italian Privacy Code.

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

Yes, the Garante manages a publicly accessible register for notifications.

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

The notification is deemed complete once the online form has been completed, or the communication is received by the Garante.

## 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 to 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 (“DPIAs”) 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”) recommends 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 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 Data Protection Officer; (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?)

Recital 47 of the GDPR provides that the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest. The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding.

As to electronic marketing in Italy, there is an obligation to inform the data subject that data are processed for such purpose, and to obtain his explicit consent which shall be recorded in writing. Consent is always required for marketing and activities and the like.

#### 9.2 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.).

Consent to automated commercial communications extends to traditional communication methods such as normal mail and phone calls which are not pre-registered. Consent to traditional means of communication does not automatically extend to automated means.

A public registry of the oppositions (opt-out) exists whereby the private citizens whose fixed line telephone number appears in the public telephone directories or similar can sign in, in order to prevent being contacted for direct phone marketing. A public registry for opting out from normal mail marketing has not been established yet.

#### 9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

The Italian Privacy Code and related rules apply to the processing of personal data, even if held abroad, carried out by anyone established

in the Italian territory or in a place subject to the Italian sovereignty, as well as to the processing of personal data carried out by anyone established in the territory of a country outside the European Union and using, for processing, instruments located in the Italian territory, unless they are used only for transit purposes within the territory of the European Union (Art. 5).

It should be noted that, however, the GDPR will have a broader scope of application, as, in general, it applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not (Art. 3).

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

The Garante is active in such enforcement as it issues guidelines and notes on the issue and as it is competent to issue decisions imposing sanctions in the event of a breach of the Italian Privacy Code, including breaches of marketing restrictions. The Garante is particularly careful in monitoring the lawfulness of profiling activities.

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

According to the national rules, the data controller shall inform the data subject of the planned communication and/or transfer to third parties, also specifying what type of entities these are. The data controller shall also obtain a separate and specific consent from the data subject.

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

Breaches of marketing restrictions are subject to the sanctions provided for at Art. 161 and *ff.* of the Italian Privacy Code, which differ on the basis of the type of data breach incurred (for instance, the absence of notice on data processing is subject to the administrative sanction of between EUR 6,000 and EUR 36,000, the maximum penalty for unlawful data processing is EUR 120,000). Unlawful processing of data can also imply criminal liability.

## **10 Cookies**

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

The Garante issued, as a result of a public consultation on 8 May 2014, a binding note on cookies, which provides that websites must ensure that when a user accesses the home page or another page of a website, a clearly visible banner must immediately appear, indicating that:

- 1) the website uses profiling cookies to send targeted advertising messages;
- 2) the website also allows the sending of “third-party” cookies, i.e. cookies installed by a different site through the website that is actually visited;
- 3) a link to more extensive information, including the one on the use of cookies sent by the website. The extensive information must contain the instructions for the data subject to refuse the installation of the cookies directly or by connection to other sites in the case of “third-party” cookies;

- 4) if browsing is continued, this implies consent to the use of cookies.

No prior consent is needed for the use of the so-called technical or analytics cookies (i.e. those used for the sole purpose of transmitting over an electronic communications network, or those used only to the extent that they are strictly necessary for the provision of a service which was specifically requested by the subscriber or user).

Use of cookies for profiling purposes is subject to the notification requirement provided for by Art. 37 of the Italian Privacy Code (see question 6.1).

Pursuant to Article 5 of the EU ePrivacy Directive, 2002/58/EC, the storage of cookies (or other data) on an end user’s device requires prior consent (the applicable standard of consent is derived from Directive 95/46/EC and, from 25 May 2018, the GDPR). For consent to be valid, it must be informed, specific, freely given and must constitute a real 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, which means that it must be essential to fulfil their request.

#### **10.2 The EU Commission intends to pass a new ePrivacy Regulation that will replace the respective national legislation in the EU Member States. The regulation is planned to come into force May 25, 2018 and will provide amended requirements for the usage of cookies. Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?**

The Commission’s proposal for a new ePrivacy Regulation, 2017/0003 (COD), provides that no consent is needed for non-privacy intrusive cookies improving internet experience (e.g. to remember shopping cart history) or cookies used by a website to count the number of visitors. For the other types of cookies, including third-party cookies, the new Regulation will render it more user-friendly as browser settings should provide for an easy way to accept or refuse tracking cookies and other identifiers.

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

The Garante issues guidelines and notes concerning cookies and it provides for related information through various channels. It is competent to issue sanction decisions and it regularly does so (see question 10.4 below).

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

The penalties for non-compliance with the data protection provisions are established at Article 161 and *ff.* of the Italian Privacy Code. These depend on the type of breach. For example, the omission or provision of unsuitable notifications can imply a sanction of between EUR 6,000–36,000; installation of cookies on users’ terminals without their prior consent can result in a sanction of between EUR 10,000–120,000; and omission or incomplete notification to the Authority can result in a sanction of between EUR 20,000–120,000.

## 11 Restrictions on International Data Transfers

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

Data transfers to 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) or the business has implemented one of the required safeguards as specified by the GDPR.

### 11.2 Please describe the mechanisms companies 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.

Transfer of personal data to the US is also possible if the data importer has signed up to the EU-US Privacy Shield Framework, which was designed by the US Department of Commerce and the EU Commission to provide businesses in the EU and the US with a mechanism to comply with data protection requirement when transferring personal data from the EU to the US.

### 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.

## 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, 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. The WP29 recommends 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, or 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, the WP29 considers 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 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.

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

The Garante issued various notes and orders concerning CCTV; in particular, the order of 8 April 2010 contains binding provisions for all those making use of CCTV and aiming at ensuring the privacy of the data subjects. In particular, the limits on use do not differ from those regulating the processing of data through other means. When CCTV is only used for personal purposes (for security of personal property, for example) the Italian Privacy Code does not apply – and no consent is needed. However, when the Italian Privacy Code applies, it is necessary to operate a balance of interests between the need to acquire the consent of the data subject and the legitimate interests for which the CCTV is based (safety, collecting evidence, etc.).

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

Employee monitoring shall always be respectful of the fundamental rights of the employees, not only with regard to privacy, but also to personal dignity and to freedom of communication and of expression. The so-called “Jobs Act” of 2015 amended Art. 4 of the “Statute of Employees”, the main employee-related legislation. The new rules make a distinction between CCTV (and distance control devices) and other kinds of monitoring.

The former is not allowed unless: i) its use is linked to the organisation or production-related needs, or it is linked to safety or to the protection of the company’s assets; and ii) there is a trade union agreement or an administrative authorisation by local labour authorities.

The restrictions under points i) and ii) are not applicable to those other tools that can allow monitoring used by the employee directly to perform his/her tasks (including smartphones, PCs, etc.) and to the apparatus to record access and presence at the workplace. The

data and information recorded by these tools can only be used for work-related purposes (which include disciplinary purposes).

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

Employees shall be provided with proper information (notification) concerning the monitoring carried out as described above. This shall include information on the existence, manner, compulsory or non-compulsory nature of the processing, on the consequence of a possible refusal to consent, the persons or entities which could process such data, the responsible data processors and the employees’ rights. In the absence of such notification to employees, the data cannot be used.

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

Trade unions (namely the internal trade union representatives (so-called RSA or RSU), or, in case of undertakings having their seats in different regions, the most representative national trade union associations) need to give their agreement for CCTV (and distance control devices). Where there is no agreement specific administrative authorisation is needed (see 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.)?**

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 EUR 20 million or 4% of worldwide turnover.

## 16 Enforcement and Sanctions

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

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
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.	N/A

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
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).	N/A
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.	N/A
Imposition of Administrative Fines for Infringements of Specified GDPR Provisions	The GDPR provides for administrative fines which can be EUR 20 million or up to 4% of the business' worldwide annual turnover of the preceding financial year.	N/A
Non-Compliance With a Data Protection Authority	The GDPR provides for administrative fines which will be EUR 20 million or up to 4% of the business' worldwide annual turnover of the preceding financial year, whichever is higher.	N/A

**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 Garante regularly issues sanctions or bans on particular data processing activities when due to their nature, methods or effects, these imply significant prejudice to the data subject. For example, the Garante very recently banned a leading mobile phone operator from continuing its massive marketing activities of sending text messages and phone calls without the prior consent of the data subjects, and even subsequent to the data subjects having expressly indicated that they did wish not to be contacted by the operator.

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

In its judgment of 1 October 2015 in case C-230/14 (confirming its findings from the Google Spain case, C-131/12), the Court of Justice of the EU stated that the concept of “establishment” pursuant to Art. 4(1)(a) of the EU Data Protection Directive 95/46/EC cannot be interpreted restrictively, but rather must be interpreted in the light of the specific nature of the economic activities concerned. The Court clarified that even carrying out of a “minimal” real and effective activity could amount to “establishment” and thus trigger the application of the law of a certain Member State.

However, as the CJEU pointed out, there is a distinction between investigative and sanctioning powers: a data protection authority cannot impose sanctions against a controller established outside its jurisdiction, but can only investigate its activities in the territory of that Member State. In such a case, the data protection authority would need to seek the cooperation of the data protection authority of the State in which the controller is established, which may carry out other investigations and actually impose sanctions. In accordance with this principle, the Italian Garante would need to contact local data protection authorities in other jurisdictions in order to seek cooperation.

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

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

The answer to this question actually depends on the legal standing (or entitlement) of the law enforcement agencies to request the e-discovery/disclosure of documents, on the type of documents requested and on the reasons for requesting. In general, it should be taken into account that, other than privacy limitations, also strict attorney-privilege limitations apply in Italy. It should also be noted that e-discovery and disclosure requests are not part of the Italian legal system.

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

The Garante has not issued any specific 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.

The Garante: (i) has been active in investigating and sanctioning telecom companies and other business carrying out aggressive telemarketing activities; (ii) is concerned about the risks connected to the amount of data circulating via social networks and the related profiling (especially after the Cambridge Analytica case); and (iii) is also active in the field of fighting cyberbullying.

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

The hot topic is currently the execution provisions that should be adopted by the Italian legislature in view of the entry into force of the GDPR, and the compliance measures and practices that businesses will have to put in place. Particularly important is the issue of the possible wide interpretation of the principle according to which data processing can be lawful when it is supported by a legitimate interest.

**Julia Holden**

Trevisan & Cuonzo Avvocati  
Via Brera, 6  
20121, Milan  
Italy

Tel: +39 2 8646 3892  
Email: [jholden@trevisancuonzo.com](mailto:jholden@trevisancuonzo.com)  
URL: [www.trevisancuonzo.com](http://www.trevisancuonzo.com)

Julia is a senior partner and jointly qualified as an English solicitor and Italian attorney. She has been practising with Trevisan & Cuonzo since its establishment in 1993. Julia has worked with Anglo-American companies and multi-national corporations for many years providing advice on all aspects of intellectual property and in particular trademark protection and enforcement including litigation, anti-counterfeiting, unfair competition and customs monitoring in diverse industries. Julia has worked with a broad range of clients.

**Benedetta Marsicola**

Trevisan & Cuonzo Avvocati  
Via Brera, 6  
20121, Milan  
Italy

Tel: +39 2 8646 3892  
Email: [bmarsicola@trevisancuonzo.com](mailto:bmarsicola@trevisancuonzo.com)  
URL: [www.trevisancuonzo.com](http://www.trevisancuonzo.com)

Benedetta joined Trevisan & Cuonzo in May 2016 having gained previous international experience at European institutions, namely the European Commission and the General Court in Luxembourg, where she specialised in trademark law working in a judge's chambers for three years. She also interned at the European Court of Human Rights and was a legal trainee in a boutique law firm in Rome. Benedetta is currently working in litigation, handling matters relating to patents, trademarks and advertising.

## Trevisan & Cuonzo

### Avvocati

Trevisan & Cuonzo's team of Data Protection and Privacy Law specialists, working in close conjunction with the intellectual property teams, regularly advises clients on privacy law issues.

The EU General Data Protection Regulation (GDPR) comes into effect on 25 May 2018 and represents a total overhaul of EU data protection law in Europe bringing potential fines for non-compliance, as well as serious risk to brand image associated with possible mistreatment of customer/client data. As a consequence, most – if not all – Italian businesses are currently reviewing and updating current internal data protection practices.

The firm's compact and well-equipped Data Protection team is fully versed in the new legislative provisions and able to guide small, medium or multinational businesses through the new privacy and data protection regulation, cross-border data transfers and information handling practices.

Given their depth of knowledge and commitment in the privacy and data protection sector, Trevisan & Cuonzo are working in close collaboration with Accomazzi Srl, well-known IT specialists with solid experience in electronic commerce, data protection and online security, to offer businesses 'ready to use' online data protection packages. These packages have been created specifically to guide Italian businesses through the new GDPR and its compliance requirements. Following simple online questionnaire methodology, this new and innovative website – which launched in April 2018 – offers its users basic formats and easily comprehensible guidelines for immediate application. The online packages automatically tailor to specific business needs. For further information, see <https://adempimenti-gdpr.it/>.



# Japan

Hiromi Hayashi



Rina Shimada



Mori Hamada & Matsumoto

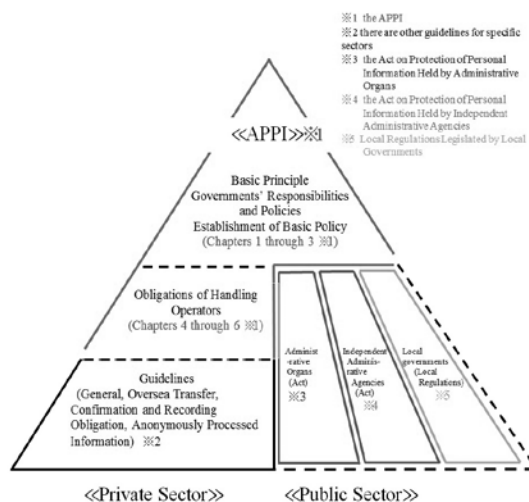
## 1 Relevant Legislation and Competent Authorities

### 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 (*jyousei*) legislated by local governments.

In addition, each Ministry regulating specific industrial sectors issues data protection guidelines for those sectors. Please see question 1.3.



On May 30, 2017, amendments to (i) the APPI, (ii) the Act on the Utilisation of Numbers to Identify Specific Individuals in Administrative Procedures (Act No. 27 of 31 May 2013, as amended; the “**My Number Act**”), and (iii) other relevant laws were fully enforced. Amendments to the APPI (the “**Amended APPI**”) include:

- Establishing the Personal Information Protection Committee (the “**PPC**”), which will supervise the enforcement and application of the APPI.
- Introducing the definition of Sensitive Personal Information.

- Introducing restrictions on transferring Personal Data to foreign jurisdictions.

The PPC was established on January 1, 2016. The Cabinet Order and the ordinance issued by the PPC (the “**PPC Ordinance**”) which provide for the details of the Amended APPI were promulgated on October 5, 2016.

#### 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 Jyohou 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. Before the amendment of the APPI, Handling Operators included all business operators using a Personal Information Database for their businesses (please see question 2.1) except for business operators with fewer than 5,000 individuals in their Personal Information Database at any time in the past six months. This exception will no longer be available upon the full effectivity of the Amended APPI. Note that administrative organs and independent administrative agencies are not Handling Operators and their data handling is regulated under the laws described in items (ii) and (iii) of the laws listed in the first paragraph above.

#### 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 15001:2006 [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 the right

of persons for their private life not to be disclosed except for 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 ("MIAC") 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 "MIAC Guidelines").

(c) **Electronic Mails**

The Act on the Regulation of Transmission of Specified Electronic Mails (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 My Number Act. It is the basic principle of this law 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?

There was no single independent regulatory authority that was responsible for implementing the previous APPI. Each Ministry that regulates specific industries was responsible for enforcing the previous APPI in that industry. In this regard, each Ministry regulating specific industries issued guidelines for those industries. The Amended APPI established the PPC which is responsible overall for implementing the APPI. The PPC issues principle guidelines of the APPI. However, in some industries, there remain specific guidelines which were issued by other ministries, such as (i) telecommunications guidelines issued by MIAC, (ii) broadcasting guidelines issued by MIAC, (iii) posting guidelines issued by MIAC, and (iv) genetic information guidelines issued by the Ministry of Economy, Trade and Industry. Further, the PPC and the Ministry of Finance 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?

Under the previous APPI, the Minister of each Ministry regulating a

specific industry was responsible for the supervision and enforcement of the APPI in that industry. Under the Amended APPI, however, 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 is a new concept introduced by the APPI Amendments (APPI, Article 2, paragraph 1). This 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, paragraph 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.

A Handling Operator is required to comply with obligations regarding Retained Personal Data under Articles 27 through 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”, which was not defined in the APPI prior to its amendment, is defined in the Amended 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 Amended 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.

#### ■ Other key definitions – please specify (e.g., “Pseudonymous Data”, “Direct Personal Data”, “Indirect Personal Data”)

- “Anonymously Processed Information” which was not defined in the APPI prior to its amendment, is defined in the Amended APPI 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).

### 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 APPI in force prior to the APPI Amendments did not explicitly provide for its application outside Japan. After the APPI Amendments, however, key provisions of the APPI apply to entities outside Japan if they receive personal information in connection with the provision of goods or services to individuals residing in Japan (APPI, Article 75).

### 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 its 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 MIAC 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 (MIAC Guidelines, Article 10).

### ■ Other key principles – please specify

#### ■ 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 when the Handling Operator (a) agrees to stop providing the 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 that (i) the provision to third parties is included in the purpose of utilisation, (ii) the items to be provided to third parties, (iii) mode of provision (e.g., by publishing a book or uploading to a website through the Internet), (iv) 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, e-mail, or any written material) (*Id.* Article 23, paragraph 2).

#### ■ 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, if a person requests a Handling Operator to notify him or 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".

#### ■ 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 provisions to third parties of, or erase, Retained Personal Data upon the request of the principal if the request has reasonable grounds (*Id.* Article 30).

However, this obligation 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 exists 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)).

■ *Other key rights – please specify*

■ **Complaint to Authorised Entities for Protection of Personal Information (*Nintei Kojin Jyohou Hogo Dantai*)**

Authorised Entities for the Protection of Personal Information (*Nintei Kojin Jyohou Hogo Dantai*) are entities authorised by the PPC to handle complaints from individuals on the handling of personal information by Handling Operators. As of April 2018, 43 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 Handling Operator, it must promptly notify the Handling Operator of the complaint and give necessary advice, investigate the circumstances pertaining to the complaint and request the Handling Operator to resolve the complaint promptly. It may, if necessary, request the Handling Operator to explain in writing or orally, or request it to submit relevant materials. The 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, 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 to 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 (i) who “opted in” to receive them, (ii) who provided the sender with their email address in writing (for instance, by providing a business card), (iii) who have a business relationship with the sender, or (iv) who 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 Anti-Spam Act on Specified Commercial Transactions also adopts the opt-in system for unsolicited marketing.

**9.2 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.

**9.3 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.

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

The MIAC 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.

**9.5 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 in itself is not illegal; however, if the list is created or shared in a manner that is in breach of the APPI, (the seller and) the purchaser may be subject to a penalty under the APPI. The maximum penalty is either imprisonment of up to one year or a fine of up to 500,000 yen (APPI, Article 83).

**9.6 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.

**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 APPI; however, if Personal Data are collected through such technology, such Personal Data is subject to the APPI.

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

Please see question 10.1.

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

Please see question 10.1.

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

Please see question 10.1.

**11 Restrictions on International Data Transfers****11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.**

Before the amendment, the APPI did not restrict the transfer of Personal Data abroad. The Amended APPI, however, imposes restrictions on the overseas transfer of Personal Information (APPI, Article 24). These restrictions include requiring the prior consent of the principals to the transfer of their Personal Information to a third party located in a foreign country. 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 at the time of writing, the PPC has not specified any foreign country as described in item (i) above. The PPC Ordinance, however, 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 companies 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.

## 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 (*Koueki Tsuchosha Hogo Hou*) prohibits employers from dismissing whistle-blowers. The 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.

**12.2 Is anonymous reporting prohibited, or strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do companies 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.

**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 at the workplace. Thus, it is recommended that employers establish internal rules prohibiting the use of company PCs and e-mail 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 14.2.

**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 representative 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) expects voluntary breach reporting.**

Under the PPC's Notification, 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 has not substantially occurred; or
- (ii) there have been minor wrong transmissions of e-mail 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.

**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) expects 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.

#### 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 500,000 yen (*Id.* Article 83). If the breach is committed by a person who is employed by an entity, such entity will be subject to the same penalty (*Id.* Article 87).

## 16 Enforcement and Sanctions

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

Investigatory Power	Civil/Administrative Sanction (under the APPI)	Criminal Sanction (under the APPI)
Personal Information Protection Committee (PPC)	(i) May require a Handling Operator to report or submit materials regarding its handling of Personal Information, enter offices or other places for investigation, make inquiries and check records or other documents (Article 40). (ii) May require an Authorised Entity for Protection of Personal Information to report regarding its activities (Article 56).	Fine of up to 300,000 yen (Article 85). If the breach is committed by a person who is employed by an entity, such entity will be subject to the same penalty (Article 87).
Same as above	May render guidance or advice to a Handling Operator (Article 41).	
Same as above	May recommend a Handling Operator to cease the violation and take other necessary measures to correct the violation (Article 42.1).	
Same as above	May order a Handling Operator to take necessary measures (Article 42.2).	Imprisonment for up to six months, or a fine of up to 300,000 yen (Article 84). If the breach is committed by a person who is employed by an entity, such entity will be subject to the same penalty (Article 87).
Same as above	Order an Authorised Entity for Protection of Personal Information to take necessary measures (Article 57).	Revoke the authorisation of an Authorised Entity for Protection of Personal Information (Article 58).

### 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 need of a court order.

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

Publicly available information does not enable the identification of specific enforcement cases by the PPC since May 2017, when the PPC became the regulator and enforcement authority of the APPI. We are aware though that the PPC has initiated enforcement actions. However, there is not enough available information to allow a description of the PPC's approach to the exercise of its powers.

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

The enforcement powers by PPC against foreign companies have been newly introduced by the Amended APPI. 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). Publicly available information does not enable the identification of specific enforcement cases against foreign companies.

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

### 17.1 How do companies 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.

In a Supreme Court decision issued in October 2017, the Supreme Court found that the breach of a right to privacy may give rise to a claim for compensation for distress caused by the leakage of Personal Information (e.g., name, birth date, address and telephone numbers). The case has been remanded to the High Court for further examination, and is still pending.

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

The PPC Ordinance is expected to be amended to specify detailed conditions for the certification of a foreign country as a country with a data protection regime with a level of protection equivalent to that of Japan, which is one of the exceptions to restrictions on overseas data transfers. Please see question 11.1.



**Hiromi Hayashi**

Mori Hamada & Matsumoto  
Marunouchi Park Building, 2-6-1  
Marunouchi Chiyoda-ku  
Tokyo 100-8222  
Japan

Tel: +81 3 5220 1811  
Email: [hiromi.hayashi@mhmjapan.com](mailto:hiromi.hayashi@mhmjapan.com)  
URL: [www.mhmjapan.com](http://www.mhmjapan.com)

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 portion of *Telecommunication in Asia* in 2005. Her other areas of practice are international and domestic transactions, takeover bids and corporate restructuring. She 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.



**Rina Shimada**

Mori Hamada & Matsumoto  
Marunouchi Park Building, 2-6-1  
Marunouchi Chiyoda-ku  
Tokyo 100-8222  
Japan

Tel: +81 3 6266 8924  
Email: [rina.shimada@mhmjapan.com](mailto:rina.shimada@mhmjapan.com)  
URL: [www.mhmjapan.com](http://www.mhmjapan.com)

Rina Shimada is an associate at Mori Hamada & Matsumoto, which she joined in 2011. Her main fields of practice include labour laws and privacy laws. In particular, she has broad experience providing advice to foreign corporations doing business in Japan. She is a graduate of Keio University (LL.B., 2007) and the University of Tokyo, School of Law (J.D., 2009), and was admitted to practise law in Japan in 2010.

## MORI HAMADA & MATSUMOTO

Mori Hamada & Matsumoto is a full-service international law firm based in Tokyo with offices in Bangkok, Beijing, Shanghai, Singapore and Yangon with a desk in Indonesia. The firm has over 400 attorneys and a support staff of approximately 450 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.

# Korea

Kwang Bae Park



Lee & Ko

Hwan Kyoung Ko



## 1 Relevant Legislation and Competent Authorities

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

In Korea, the collection and processing of personal data is governed by the Personal Information Protection Act (“PIPA”), the comprehensive general data protection law.

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

The Criminal Code makes it a criminal offence for any party to open any letter, document or drawing that is sealed or designed to be secret, or to learn the contents of any such letter, document, drawing, or special recording medium such as electronic records by employing technical means.

The Communications Privacy Protection Act (“CPPA”) makes it a criminal offence for any party to acquire or record the contents of any “transmission or reception of all kinds of sounds, words, symbols or images by wire, wireless, fibre-optic cable or other electromagnetic system, including telephone [and] e-mail”, except with the consent of the party concerned.

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

There are a number of other sector-specific laws which include:

- the Act on Promotion of Information and Communications Network Utilisation and Information Protection (the “Network Act”), which governs information and communications service providers;
- the Utilisation and Protection of Credit Information Act (the “Credit Information Act”) and the Electronic Financial Transactions Act, both of which protect consumer financial information; and
- the Act on the Protection and Use of Location Information (the “Location Information Act”), which protects personal location information.

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

- MOIS (Ministry of the Interior and Safety): enforces the PIPA and issues formal interpretations thereon.

- PIPC (Personal Information Protection Commission): shapes data protection policy while assessing the enactment/ amendment of laws and administrative measures relating to the protection of personal information.
- KCC (Korea Communications Commission): enforces the Network Act and issues formal interpretations thereon.
- KISA (Korea Internet & Security Agency): performs tasks delegated to it by the MOIS, KCC and PIPC.
- FSC (Financial Services Commission): enforces the Credit Information Act and issues formal interpretations thereon.

## 2 Definitions

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

#### ■ “Personal Data”

Under the PIPA, “personal data” is defined as “any data relating to a living person, and from which the individual can be identified through one’s name, resident registration number, or visual image and so on (including information from which, if not by itself, can be easily combined with other information to identify a specific individual)”.

#### ■ “Processing”

Under the PIPA, “processing” is defined as “the collection, generation, recording, storage, retention, processing, editing, search, outputting, rectification, restoration, use, provision, disclosure or destruction of personal information or any other action similar to any of the foregoing”.

#### ■ “Controller”

Under the PIPA, “data controller” means “a public institution, corporate body, organisation, or individual who processes information directly or via another person to administer personal information files (defined as “a collection of personal information in which personal information is systematically organised pursuant to certain rules for easy search/use”) as part of its/his/her duties”.

The Network Act regulates the processing of personal data of users by information and communications service providers (“ICSPs”) which are defined as “(1) telecommunications business operators under the Telecommunications Business Act and (2) commercial providers of information services that utilise telecommunications services provided by a telecommunications business operator”.

Under the Credit Information Act, the concept of “credit information provider/user” is similar to that of a controller

and means “a person who provides any third party with credit information obtained or produced in relation to his/her own business for purposes of commercial transactions, such as financial transactions with customers, or who has been continuously supplied with credit information from any third party to use such information for his/her own business, or other persons corresponding thereto”.

#### ■ “Processor”

Under the PIPA, an “outsourced processor” means “a public institution, corporate body, organisation, or individual who processes personal information entrusted by and for the benefit of the data controller”.

#### ■ “Data Subject”

Under the PIPA, a “data subject” means “a person who can be identified by processed information and therefore is the subject of the given piece of information”.

Under the Network Act, a “user” means “a person who uses information and communications services provided by an ICSP”.

#### ■ “Sensitive Personal Data”

Under the PIPA and regulations issued thereunder, “sensitive personal data” means any information on the ideology, creed, membership of a labour union or political party, political views, health, sexual preferences, bio-data, and criminal records as defined under the Act on the Lapse of Criminal Sentences.

#### ■ “Data Breach”

Under the Standard Guidelines for the Protection of Personal Data, a “personal information leak” is defined as “the data controller’s involuntary loss of control of the personal data of data subjects or the allowance of access thereto by unauthorised persons that is not pursuant to an applicable law or regulation”.

#### ■ Other key definitions – please specify (e.g., “Pseudonymous Data”, “Direct Personal Data”, “Indirect Personal Data”)

- Particular Identification Data: unique identifiers assigned to each individual as prescribed by law or regulation such as resident registration numbers (“RRNs”), driver’s licence numbers, passport numbers, and alien registration numbers.
- Pseudonymised Data: although this concept is not currently defined under the PIPA, the Korean government recently announced that it would seek to introduce this concept (as defined under the EU data protection regime) by amending privacy laws.

### 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?

Although Korean data protection laws do not expressly provide as such, regulators in Korea are of the position that Korean data protection laws should apply to any foreign companies that process the personal data of Korean citizens.

### 4 Key Principles

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

##### ■ Transparency

The data controller shall disclose matters related to the

processing of personal data (e.g., through a privacy policy), and guarantee the data subject’s right to access his/her personal data.

##### ■ Lawful basis for processing

The data controller must lawfully and justly collect personal data.

##### ■ Purpose limitation

The data controller shall make clear the purposes of processing personal data, properly process the personal data within the scope of such purposes, and shall not use the personal data for any other purpose.

##### ■ Data minimisation

The data controller shall collect only the minimum amount of personal data that is necessary for carrying out its stated purposes and the data controller shall bear the burden of proving that its collection of personal data adheres to this minimum necessary standard.

##### ■ Proportionality

The data controller shall properly process the personal data within the scope of the purpose necessary for processing the personal data.

##### ■ Retention

The data controller shall safely manage the personal data by taking into consideration the likelihood/risk of the data subject’s rights being infringed upon based on the method and type of processing.

The data controller shall implement managerial, technical, and physical security measures necessary to ensure the safety of personal data and destroy personal data without delay as soon as it is no longer necessary.

##### ■ Other key principles – please specify

Restriction on the processing of RRNs: Under the PIPA, data controllers may not collect or use RRNs except in the following cases:

1. the processing of RRNs is specifically required or permitted by a law or regulation; or
2. there exists a clear and urgent need to protect the life, physical or economic interest of the data subject or a third party.

## 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 is entitled to request access to his/her personal data that is being processed by a data controller and the data controller must comply with the data subject’s request within 10 days of receiving such request unless it has a justifiable reason.

##### ■ Right to rectification of errors

Once the data subject accesses his/her personal data, such data subject has the right to request the data controller to rectify his/her personal data and in such cases, the data controller is required to review the subject personal data without delay and provide notice of the status/results of the data subject’s request after taking necessary measures such as rectification.

##### ■ Right to deletion/right to be forgotten

Once the data subject accesses his/her personal data, such data subject has the right to request the data controller to delete his/her personal data and in such cases, the data controller is required to review the subject personal data without delay

and provide notice of the status/results of the data subject's request after taking necessary measures such as deletion.

■ **Right to object to processing**

A data subject is entitled to request the suspension of the processing of his/her personal data that is being processed by a data controller and the data controller must, without delay, suspend processing of some or all of the data subject's personal data unless it has a justifiable reason.

■ **Right to restrict processing**

Individuals do not appear to have the right to restrict processing. However, the Network Act provides that ICSPs, upon receiving requests from users to rectify errors in their personal data, must refrain from using or providing such personal data until necessary measures have been taken.

■ **Right to data portability**

There is no right to data portability under Korean law, but discussions have taken place to introduce this right through future legislative amendments.

■ **Right to withdraw consent**

Although the PIPA does not expressly provide the right to withdraw consent, it is widely understood that this right is implied thereunder because data subjects are entitled to choose whether to provide consent and to determine the scope of such consent.

■ **Right to object to marketing**

When obtaining consent for the processing of personal data for the purpose of promoting goods/services or soliciting the sale thereof, the data controller shall provide clear notice of such purpose to data subjects and the data controller may not deny the subject goods/services to a data subject that has refused his/her consent to the such purpose.

■ **Right to complain to the relevant data protection authority(ies)**

Any person who suffers infringement of rights or interests relating to his/her personal data when such personal data is processed by a data controller may report such infringement to KISA. Any person, who wants a dispute over personal data to be mediated, may apply for mediation of such dispute to the Dispute Mediation Committee.

■ *Other key rights – please specify*

Liability related to the processing of personal data: under the PIPA, a data controller may not avoid liability for damages arising from the leakage or misuse of personal data it has processed for its own benefit unless it can establish that such leakage or misuse is not attributable to its intentional or negligent act or omission. In the event a data subject suffers damages due to the loss, theft, leakage, falsification, alteration, or damage of his/her own personal data caused by an intentional or grossly negligent act or omission of the data controller, a court may award punitive damages of up to treble the amount of suffered damages. The PIPA also provides that statutory damages of up to KRW 3 million may be awarded under certain conditions even if the data subject is unable to prove the actual amount of suffered damages.

## 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 (excluding public institutions) are not subject

to any registration/notification obligations when processing personal data. However, businesses handling specific information (which typically include personally identified/identifiable information) may become subject to certain registration/notification obligations for their businesses.

Any person who intends to operate a location information business must obtain permission from the KCC after indicating his/her trade name, location of the main office, type and description of the relevant location information business, and major business facilities, including location information systems. Any person who intends to operate a location-based service business must file a report with the KCC indicating his/her trade name, location of the main office, type of relevant location-based service business, and major business facilities, including location information systems.

Under the Credit Information Act, any person who intends to operate a credit inquiry rating service, credit investigation service, etc. (which typically handle credit information) must obtain permission from the FSC.

**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)?**

Any person who intends to obtain permission to operate a location information business shall file an application form that includes detailed information on the following in addition to a business plan: 1) general information regarding the applying corporation; 2) a sales plan; and 3) a technical plan.

Any person who intends to file a report as a location-based service business shall include the following documents: 1) a business plan; 2) documents describing and indicating the location of major business facilities; and 3) documents confirming the implementation of security measures for location information.

**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 refer to our response to 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)?**

The Location Information Act does not expressly prohibit foreign legal entities from registering as a location information business or reporting as a location-based service business. However, in practice, we are not aware of any cases where a foreign legal entity has actually conducted such registration or reporting without establishing a Korean 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)?**

Please refer to our response to question 6.2.



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

Any person that operates a location information business without obtaining registration may be subject to imprisonment of up to five (5) years or a fine of up to KRW 50 million.

Any person that operates a location-based service business without filing a report may be subject to imprisonment of up to three (3) years or a fine of up to KRW 30 million.

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

This is not applicable in Korea.

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

This is not applicable in Korea. For your reference, there is no expiration date for registrations/notifications.

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

Please refer to our response to question 6.1.

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

Yes, but the relevant website is only provided in Korean.

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

This is not applicable in Korea.

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

Obtaining approval as a location information business typically takes around two months, but may take longer under certain circumstances.

**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 PIPA, appointment of a Data Protection Officer ("DPO") is mandatory.

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

Failure to appoint a DPO may result in an administrative fine of up to KRW 10 million.

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

A data controller may not permit a DPO to suffer any disadvantages when performing his/her duties without a justifiable reason.

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

The PIPA does not expressly prohibit the appointment of a single DPO to cover multiple entities. However, we are not aware of any cases where a DPO has been appointed as such.

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

The PIPA provides that an owner of a business, representative director, executive officer, or (if there are no executive officers) the head of the department responsible for handling tasks related to the processing of personal data.

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

The DPO is responsible for the overall management of tasks related to the processing of personal data and performs the following specific tasks: 1) establishes and executes a personal data protection plan; 2) carries out routine check-ups and improves the conditions and practices concerning the processing of personal data; 3) responds to relevant complaints, and provides redress to data subjects who have incurred damages from such processing; 4) establishes an internal control system to prevent leakages, misuse and abuse of personal data; 5) establishes and implements education programmes; 6) protects, manages and supervises personal data files; 7) establishes, modifies and executes a privacy policy; 8) manages materials relating to the protection of personal data; and 9) destroys personal data whose retention period has expired or for which the purposes of processing have been achieved.

**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 have to be registered or notified.

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

Yes. In the event a DPO has been appointed or replaced, confirmation of such fact and the name, department, and contact information of relevant individuals must be disclosed in the privacy policy.

**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. Under the PIPA, in order to outsource the processing of

personal data to third parties, data controllers are required to enter into a written data processing agreement with the outsourced processor that includes the following matters stipulated by law: 1) restrictions on the processing of personal data beyond the purposes of the outsourced tasks; 2) matters related to technical and managerial security measures for the protection of personal data; 3) the purposes and scope of the outsourced tasks; 4) restrictions on the subcontracting of the outsourced tasks; 5) measures to ensure the security of personal data such as restriction of access; 6) matters related to supervision of the outsourcing of the processing of personal data; and 7) matters related to the data controller's liability for damages that may arise due to violations committed by outsourced 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.)?**

Please refer to our response to question 8.1.

## 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 the Network Act, the transmission of for-profit advertisements through an electronic medium (e.g., telephone, mobile phone, fax, email, etc.) requires the express prior consent of recipients. Additionally, the Network Act provides for certain information that must be included in for-profit advertisements and specifies certain acts that the sender is prohibited from engaging in.

**9.2 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.)**

A telemarketer, as defined under the Act on Door-to-Door Sales, Etc., may engage in telemarketing without obtaining the prior consent of recipients in cases where notice of the sources where personal data is collected is provided orally to such recipients.

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

Although the above restrictions do not appear to be typically enforced on marketing sent from other jurisdictions, we are aware that the KCC has joined UCENET (Unsolicited Communications Enforcement Network), an international spam enforcement cooperation organisation, and is seeking to increase cooperation with other foreign enforcement agencies.

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

Among Korean regulators, the KCC and KISA actively enforce illegal spamming. KISA operates an illegal spam response centre

that reviews illegal spam incidents upon receiving complaints and may request other enforcement agencies to conduct investigations and impose sanctions.

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

Generally, no. However, the PIPA requires a data controller to obtain consent for the provision of personal data to third parties after providing data subjects with notice of certain matters regarding the provision. For your reference, the Supreme Court of Korea found that the defendant, a large retailer that operated a chain of discount stores, was criminally liable for violating the PIPA because it had acquired personal data or obtained consent for the processing of personal data by fraud or other unlawful means when it misled customers into believing they were participating in a promotional giveaway event and collected personal data that was unrelated to the event that was later sold to third parties for profit.

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

Under the Network Act, any person that sends marketing communications through prohibited means (e.g., using measures to avoid or interfere with a recipient's refusal to receive or withdraw his/her consent to the receipt advertising information, using measures to automatically generate a recipient's contact information, etc.) or containing prohibited content (e.g., gambling, illegal drugs, etc.) may be subject to imprisonment for up to one year or a fine of up to KRW 10 million.

## 10 Cookies

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

The law does not prescribe any particular rules relating to the use of cookies or equivalent technologies. To the extent any such information is deemed personal data, rules under the PIPA and the Network Act will apply. For your reference, ICSPs are required under the Network Act to disclose in their privacy policies information on the installation of applications (e.g., cookies) that automatically collect personal data and the methods on how to avoid such installation.

**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 Korea.

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

No enforcement action has been taken in relation to cookies.

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

This is not applicable in Korea.

## 11 Restrictions on International Data Transfers

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

Korean law provides separate requirements for the provision of personal data ("Provision") and the outsourcing of the processing of personal data ("Outsourcing"). Specifically, a Provision refers to cases where a data transfer is conducted for the benefit and business purpose of the transferee, whereas an Outsourcing refers to cases where a data transfer is conducted for the benefit and business purpose of the transferor.

Under the PIPA, if a data controller conducts a Provision to a foreign-based entity, it is required to obtain the consent of data subjects after providing notice of matters prescribed by law. However, if a data controller conducts an Outsourcing to a foreign-based entity, the data controller is not required to obtain such consent.

Under the Network Act, an ICSP that conducts a Provision or an Outsourcing to a foreign-based entity will be subject to notice and consent requirements. However, an ICSP is not required to obtain the consent of users if an Outsourcing (i) is necessary for the provision of service to users, (ii) enhances the convenience of the users, and (iii) information such as the outsourced tasks and the identity of outsourced processors has been disclosed through the ICSP's privacy policy.

### 11.2 Please describe the mechanisms companies 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.).

Personal data is normally transferred abroad after the data subjects' consent.

### 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/notification requirements.

## 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 are no data protection rules governing whistleblowing, so the PIPA will be applicable as the general data protection law.

However, it may be worth noting that the Protection of Public Interest Whistleblowers Act ("PPIWA") provides for certain measures to be taken to ensure the secrecy and confidentiality of "public interest whistleblowers". "Public interest whistleblowing"

is defined as "reporting, petitioning, informing or accusing that a public interest violation (i.e., an act that infringes on the health and safety of the public, the environment, or consumer interests and fair competition, etc.) has occurred or is likely to occur, or the providing of information during an investigation of an alleged public interest violation". Any person may report a public interest violation to the relevant organisation representative, an investigative agency, etc.

A public interest whistleblower must file a written report containing the personal details of the whistleblower and identity of person that is alleged to have committed a public interest violation. Under the PIPA, a public interest whistleblower is permitted to report the personal data of a person that is alleged without such person's consent because such provision is specifically required under the PPIWA.

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

No, anonymous reporting is not prohibited. However, under the PPIWA, a public interest whistleblower must state his/her personal details when filing a written report in order to be afforded protection thereunder.

## 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)?

In general, there is no registration/notification requirement or need to obtain prior approval from the data protection authorities in order to use CCTV in Korea. However, a notice sign stating the following information must be placed in cases where CCTV is installed in a publicly disclosed location: installation location and purpose of installation; field of view and recording time; person in charge of managing the CCTV and his/her contact information; and name (job title) of person in charge, name of company, and contact information of the outsourced third party (if applicable).

The prior consent of data subjects is required under the PIPA in order to lawfully install and operate CCTV in undisclosed locations.

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

If CCTV data can be used to identify specific individuals, then it will be regarded as personal data under the PIPA and the collection/use thereof will be subject to consent requirements thereunder. CCTVs in undisclosed locations may only be installed and operated with the prior consent of data subjects.

In principal, the installation and operation of CCTV in a publicly disclosed location is prohibited under Korean law except in the following cases: where specially permitted by a law or regulation (e.g., parking lots, kindergartens, elementary schools, airports, etc.); where necessary to prevent crime or provide assistance to an investigation; where necessary for the safety of facilities or to prevent fires; where necessary for traffic regulation; and where necessary to collect, analyse, and provide traffic information.

## 14 Employee Monitoring

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

In general, employee monitoring is only permitted in cases where necessary consent has been obtained under the PIPA or CPPA. Please note, however, that in a case where a company conducted employee monitoring based on reasonable suspicions that the confidential information of the company was being leaked, the Supreme Court of Korea found that the company was justified in conducting employee monitoring.

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

Yes, consent is required. The CPPA prohibits the wiretapping of a device without the consent of the party concerned. Also, there may be the issue of whether there was an invasion of such individual's privacy in violation of the Criminal Code and the Network Act, and as employee monitoring will be deemed to be the collection of personal data, consent for the collection and use of personal data must be obtained in accordance with the PIPA. As the PIPA prescribes detailed rules on how to obtain the consent thereunder, it is necessary to obtain consent pursuant to the PIPA.

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

The Act on the Promotion of Workers Participation and Cooperation provides that the work council shall be consulted with in order to "install employee surveillance systems/facilities 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.)?

Under the PIPA and Network Act, all data controllers (including data processors) are required to ensure the security of personal data. The Standards of Personal Information Security Measures, an implementing regulation issued under the PIPA, and the Standards of Technical and Administrative Safeguards for Personal Information, an implementing regulation issued under the Network Act, provide detailed information on security measures that must be implemented.

### 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) expects voluntary breach reporting.

Yes. Under the PIPA, the MOIS must be notified if a data breach occurs that involves the personal data of 1,000 or more data subjects. Such notice should contain: the items of personal data that have been

leaked; the time when the personal data was leaked and reasons for the leak; information on measures to be taken by the data subject to minimise damages; countermeasures taken by the data controller and procedures for remedying damages to the data subject; and contact information for the data controller's department responsible for reporting damages to the data subject. The PIPA provides that notification should be made "without delay", which is interpreted as meaning "within five days" under regulatory guidelines.

In cases where the Network Act is applicable, the KCC must be notified, without delay, in any event within 24 hours, upon the occurrence of a data breach unless there is a justifiable reason (there is no threshold of "1,000 or more data subjects"). The information that must be included when providing notification is identical to that provided by the PIPA.

### 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) expects voluntary breach reporting.

Yes, there is a legal requirement to report data breaches to affected data subjects. The information that must be included is identical to the information required when providing notification to data protection authorities. However, where the PIPA is applicable, data subjects must be notified even if the data breach affects fewer than 1,000 data subjects.

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

The maximum penalties that may be imposed on each entity are as follows:

- A data controller that fails to implement security measures discussed in our response to question 15.1: an administrative fine of up to KRW 50 million.
- The person responsible for a failure to implement security measures discussed in our response to question 15.1 which leads to the loss, theft, leakage, falsification, alteration, or damage of personal data: imprisonment of up to two years or a fine of up to KRW 20 million.
- A data handler whose legal representative or employee is responsible for such failure to implement the security measures above: a fine of up to KRW 20 million.
- A data controller who is at fault for the leakage of RRNs it has been processing: a penalty surcharge of up to KRW 500 million.

## 16 Enforcement and Sanctions

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

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
MOIS	Yes	No
KCC	Yes	No
Financial Services Commission (FSC)	Yes	No
Public Prosecutors	No	Yes



### 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 MOIS, KCC and FSC possess discretionary authority to issue bans (i.e., corrective orders) pursuant to applicable laws and such 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.

Data protection authorities tend to exercise their powers actively. Specifically, the authorities will investigate reported violations and leakages of personal data and may also investigate companies within a particular industry to identify and punish violations.

On September 8, 2017, the KCC imposed stern administrative sanctions (a penalty surcharge of KRW 301 million, an administrative fine of KRW 25 million, etc.) against an operator of a hospitality app for a data breach.

Additionally, on December 6, 2016, the KCC imposed a record-high penalty surcharge of KRW 4.48 billion and an administrative fine of KRW 25 million on a leading online shopping mall operator in Korea, for a data breach that resulted in the leak of over 25 million items of customers' personal data.

Recently, the MOIS imposed administrative sanctions after conducting several industry-wide inspections including:

- Inspection of industries closely related to the lives of ordinary citizens (cosmetics, automobile, etc.) (July 2017).
- Inspection of hospitals conducting health examinations and dental hospitals (May 2017).
- Inspection of businesses in the sports industry such as golf courses and baseball teams (March 2017).

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

Yes. Most notably: 1) the KCC requested Facebook to upgrade its services based on the fact that they lacked the necessary protection for personal data (e.g., Facebook's notification and consent procedures were found to be inadequate), and Facebook announced its plans to improve upon its services before it was actually sanctioned by the KCC; and 2) the KCC also imposed penalty surcharges on Google Inc. (based in the US) for collecting personal data without obtaining the data subject's consent in connection with Google's provision of street view services.

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

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

Korean laws do not provide any particular rules on third-country e-discovery or law enforcement requests. Therefore, personal data that is provided to a foreign regulatory authority or judicial authority will be treated the same as personal data that is provided to a third party.

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

There has been no relevant guidance issued.

## 18 Trends and Developments

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

Recently, the focus of enforcement has been expanded to security measures for personal data. As discussed in our response to question 16.3, the KCC has recently imposed stern administrative sanctions for data breaches. Additionally, on August 30, 2017, the KCC issued administrative warnings against 2,462 online businesses that were found to have violated provisions of the Network Act related to the disclosure of a privacy policy, notice and consent requirements, and issued corrective orders. Further, the KCC announced that it would directly impose administrative sanctions such as fines for any similar violations in the future.

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

In July 2016, the Korean government published the Guidelines on Personal Information De-identification Measures in order to specify the criteria, procedures, and methods of de-identification measures necessary for utilising big data. However, the practical usefulness of the guidelines has faced increasing criticism because they lack binding legal effect. In connection to this, various civic organisations referred KISA and three other specialised government agencies to investigative authorities in November 2017 for violating provisions of Korean privacy laws when such government agencies de-identified and returned over 340 million items of personal data that had been entrusted to them by 20 private companies. In February 2018, a joint panel of experts from the public sector, civic organisations, and the private sector agreed to seek the amendment of privacy laws to establish legal grounds for the processing of pseudonymised data (as defined under the EU data protection regime) at a Hackathon event hosted by the Presidential Committee on the Fourth Industrial Revolution.

**Kwang Bae Park**

Lee & Ko  
Hanjin Building 63 Namdaemun-ro  
Jung-gu Seoul 04532  
Korea

Tel: +82 2 772 4343  
Email: [kwangbae.park@leeko.com](mailto:kwangbae.park@leeko.com)  
URL: [www.leeko.com](http://www.leeko.com)

Kwang Bae PARK is a partner and leader of the Technology, Media & Telecommunications Practice Group at Lee & Ko. He has consistently represented and advised the various telecommunications and IT companies for more than 10 years since 1991, with a focus on various issues in the field of all TMT areas, including mobile and regulatory issues in internet services, such as issues on privacy, internet contents, and internet advertisements.

Mr. Park also serves on various committees such as the Regulation Review Committee (Ministry of Science and ICT), the Joint Task Force for EU Adequacy Assessment (Ministry of the Interior and Safety), etc. Also, he was rewarded and recognised as a "Leading Telecoms & Media Lawyer" (*The International Who's Who Legal*, 2014–2017), a "Ranked Lawyer" (Band 1) (*Chambers Asia Pacific*, 2015–2017), etc.

Mr. Park holds an LL.B. from Seoul National University and an LL.M. from Georgetown University Law Center. He is admitted to the New York and Korean Bars.

**Hwan Kyoung Ko**

Lee & Ko  
Hanjin Building 63 Namdaemun-ro  
Jung-gu Seoul 04532  
Korea

Tel: +82 2 2191 3057  
Email: [hwankyung.ko@leeko.com](mailto:hwankyung.ko@leeko.com)  
URL: [www.leeko.com](http://www.leeko.com)

Hwan Kyoung KO is a partner in the Technology, Media & Telecommunications Practice Group. He is a leading expert in the areas of telecommunications, IT, data privacy, and Fintech. He has advised numerous government agencies, including the Financial Services Commission and the Korea Communication Commission, on data protection and also served as a member of the Big Data Task Force. Mr. Ko has also been involved in efforts to promote the Big Data industry in Korea as witnessed by his participation in a recent Hackathon event hosted by the Presidential Committee on the Fourth Industrial Revolution.

Mr. Ko is a recipient of the 2016 Minister of the Interior and Safety's Award (in the data protection sector) and the 2014 KISA President's Award for Personal Data Protection.

Mr. Ko holds a B.A. from Korea University and an LL.M. from Georgetown University Law Center. He is admitted to the New York and Korean Bars.



Lee & Ko's evolution as the premier law firm in Korea parallels in many ways the solid economic development of the country for more than 40 years following its founding in 1977.

Our firm is one of the top law firms in Korea that is recognised for expertise in all major practice areas, which includes over 30 specialised practice groups, and that is consistently acclaimed over the years as one of the leading firms in Asia by internationally respected legal publications and league tables.

Also, Lee & Ko has a global client base that includes domestic conglomerates to multinational corporations in many different industries. We have an unrivalled list of leading clients from the US, EU, China, Japan and more as well as high-profile start-up high-tech companies. Our global reach is a result of our Korean-licensed lawyers with outstanding foreign-language capabilities working together with our experienced foreign-licensed lawyers.

# Luxembourg

Véronique Hoffeld



Loyens & Loeff Luxembourg S.à r.l.

Florence D'Ath



## 1 Relevant Legislation and Competent Authorities

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

From 25 May 2018, the principal data protection legislation in the EU will be Regulation (EU) 2016/679 (the “**General Data Protection Regulation**” or “**GDPR**”). The GDPR repeals Directive 95/46/EC (the “**Data Protection Directive**”) and leads to increased (though not total) harmonisation of data protection law across the EU Member States.

In Luxembourg, a draft bill N°7184 was introduced on 12 September 2017 in order to complement the GDPR. It is likely to enter into effect on 25 May 2018.

The draft bill N°7184 is to repeal the law of 2 August 2002 on the protection of individuals as regards the processing of personal data (hereafter “**Law of 2002**”), which is currently the principal data protection legislation in Luxembourg.

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

The Law of 30 May 2005 for the protection of persons with regard to the processing of personal data in the electronic communications sector (as amended by different laws) implements nationally 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 that would harmonise the applicable rules across the EU.

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

There are three sectorial laws, which notably impact data protection in Luxembourg:

- the Law of 24 July 2014 (which establishes rules as to the processing of health data);
- the Law of 23 July 2016 (which sets out relevant data protection standards as to criminal data); and
- the Law of 2002 (which is the principal data protection legislation in Luxembourg and notably sets out rules related to employee monitoring).

Employee monitoring is also regulated by the provisions of the Luxembourg Labour Code.

It is very likely that these laws will be amended, in view of the implementation of the GDPR and the draft bill N°7184.

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

In Luxembourg, the National Commission for Data Protection (hereafter “**CNPD**”) verifies the legality of the processing of personal data, ensures the respect of fundamental rights with regard to data protection and privacy, and issues recommendations.

In view of the GDPR and according to the draft bill N°7184, the CNPD will be the supervisory authority in Luxembourg.

## 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.
- *Other key definitions – please specify (e.g., “Pseudonymous Data”, “Direct Personal Data”, “Indirect Personal Data”).*  
There are no other specific key definitions.

### 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 persons located in the EU in relation to: (i) the offering of goods or services (whether or not in return for payment) to persons located in the EU; or (ii) the monitoring of the behaviour of persons located in the EU (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 persons located in the EU (to the extent such behaviour takes place in the EU).

It is likely that the national law which will complement the GDPR may qualify as an overriding mandatory rule. In that sense, it is likely to apply to businesses established in other jurisdictions.

### 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 interest 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 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 CNPD, if the data subjects live in Luxembourg or the alleged infringement occurred in Luxembourg.

#### ■ **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?

Under the Law of 2002, processing activities generally have to be notified to the CNPD prior to their implementation. Some specific processing activities, however, such as employee monitoring, may not be carried out without having been explicitly authorised by the CNPD.

The draft bill N°7184, following the GDPR, plans to move from *ex ante* controls to *ex post* controls. In that sense, the notification and approval regime is likely to be abolished.

It should however be noted that the Luxembourg Chamber of Employees has issued several opinions against the deletion of the prior authorisation mechanism with regard to data processing for monitoring purposes at the workplace. It is therefore unclear whether or not businesses will still have to notify or require an authorisation for processing activities related to employee surveillance.

### 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 Law of 2002, the CNPD provides templates of notification forms, which, according to the draft bill N°7184, will no longer be necessary, as of 25 May 2018.

### 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?**

According to the draft bill N°7184, there will be no regime of prior authorisation by the CNPD.

However, a prior consultation of the CNPD may be required, if the processing activity is likely to result in a “high risk” to the rights and freedoms of the data subjects concerned (see section 14).

**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; 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 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 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 to his or her role as a Data Protection Officer?**

The appointed Data Protection Officer should not be dismissed or penalised for performing their tasks, he or she is legally protected by the GDPR against unfair termination or unfair dismissal. The Data Protection Officer 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 (“WP29”) recommends 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 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 Data Protection Officer; (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?)

Following the Law of 30 May 2005 (see question 1.2), the sending of electronic direct marketing is in principle prohibited, unless individuals have given their prior consent.

As an exception, where a supplier/service provider obtains from its existing customers (individuals) their electronic contact details, that supplier/service provider may advertise similar products or services, on the condition that individuals are given the opportunity to object, free of charge and in an easy manner, to such communication, both initially and on the occasion of each subsequent communication.

Following the Law of 30 May 2005, this general prohibition not to send marketing emails without the prior consent of the person concerned does not apply to legal persons.

### 9.2 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.).

Following the Law of 30 May 2005, direct marketing by telephone is only permitted with the individual's prior consent. This prohibition does not apply to legal persons.

### 9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

There is no consensus on that matter but one could consider the Law of 30 May 2005 as an overriding mandatory rule. In that sense, it would apply to marketing sent from other jurisdictions.

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

Following the Law of 30 May 2005, the CNPD is active in the enforcement of breaches to marketing restrictions. Such a breach is punishable by a fine from EUR 251 to EUR 125,000 and/or eight days' imprisonment.

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

The purchasing of marketing lists is not prohibited as such. However, under the Law of 30 May 2005, direct marketing is only permitted with the individual's prior consent. In that sense, one could only purchase marketing lists from third parties, on the condition that individuals on that list have consented beforehand to be contacted by the legal person purchasing such a list. Furthermore, individuals should be given the possibility to opt-out.

### 9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

Following the Law of 30 May 2005, sending marketing communications in breach of applicable restrictions is punishable by a fine from EUR 251 to EUR 125,000 and/or eight days' imprisonment.

## 10 Cookies

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

The Law of 30 May 2005 for the protection of persons with regard to the processing of personal data in the electronic communications sector (as amended by different laws) 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 Directive 95/46/EC and, from 25 May 2018, the GDPR). For consent to be valid, it must be informed, specific, freely given and must constitute a real 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, which means that it must be essential to fulfil their request.

**10.2 The EU Commission intends to pass a new ePrivacy Regulation that will replace the respective national legislation in the EU Member States. The regulation is planned to come into force May 25, 2018 and will provide amended requirements for the usage of cookies. Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?**

The current national legislation does not refer to any distinction between different types of cookies.

Considering that the new ePrivacy Regulation has not yet been passed, there is currently no draft bill concerning such a distinction in Luxembourg.

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

The CNPD has not yet issued any guidance on the use of cookies, nor taken enforcement action in relation to cookies.

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

Under the Law of 30 May 2005, the maximum penalties for breaches of cookie restrictions are a fine of EUR 125,000 and/or imprisonment of eight days.

## 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) or the business has implemented one of the required safeguards as specified by the GDPR.

**11.2 Please describe the mechanisms companies 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.

Transfer of personal data to the US is also possible if the data importer has signed up to the EU-US Privacy Shield Framework, which was designed by the US Department of Commerce and the EU Commission to provide businesses in the EU and the US with a mechanism to comply with data protection requirements when transferring personal data from the EU to the US.

**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 GDPR, it is true that some data transfers will require registration/notification to the authorities, as summarised in the table below:

No prior approval nor notification required	Prior approval	Notification
Adequate Jurisdiction (white list)	Code of conduct*	
Binding and enforceable instrument between public authorities or bodies	Certification mechanism*	
Standard Contractual Clauses adopted by the EU Commission or by the supervisory authority	BCRs	
Derogations (article 49 of the GDPR) for transfers based on: <ul style="list-style-type: none"> <li>■ explicit consent;</li> <li>■ performance of a contract;</li> <li>■ conclusion of a contract;</li> <li>■ important reasons of public interest;</li> <li>■ the establishment, exercise or defence of legal claims;</li> <li>■ the protection of the vital interests of the data subject; or</li> <li>■ a register and intended to provide information to the public and open to consultation</li> </ul>	Contractual clauses	Derogations (article 49 of the GDPR) for transfers which: <ul style="list-style-type: none"> <li>■ are not repetitive;</li> <li>■ concern only a limited number of data subjects;</li> <li>■ are necessary for the purposes of compelling legitimate interests pursued by the controller; or</li> <li>■ whose circumstances have been assessed; and</li> <li>■ provide suitable safeguards (article 49 of the GDPR)</li> </ul>
	Provisions inserted into administrative arrangements	

\*Under the GDPR, codes of conduct, which are presented by associations or bodies representing categories of controllers or processors, only have to be approved once by the supervisory authority. The same applies to certification, which is given to a controller or processor for a period of three years.



**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. The WP29 recommends 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, or 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, the WP29 considers 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 put in place 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.

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

To our current knowledge, there are no limits, other than the one provided for in the GDPR, on purposes for which CCTV data may be used in Luxembourg.

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

For the time being, article L. 261-1 of the Labour Code and the Law of 2002 regulate employee monitoring in Luxembourg. Employee monitoring is only authorised for specific purposes as laid down in article L. 261-1 of the Labour Code, e.g., to ensure the security and health of employees, protection of the employer's property, control of the production process, or the organisation of the mobile working schedule. The employer must seek a prior authorisation from the CNPD. The employer is also required to inform employees as well as the staff delegation (if any) prior to the implementation of such a monitoring system.

The draft bill N°7184, which shall repeal the Law of 2002, does not introduce additional restrictions on employee monitoring than those generally set out within the GDPR and article L. 261-1 of the Labour Code.

However, the Luxembourg Chamber of Employees has issued several opinions against the deletion of the CNPD prior authorisation mechanism with regard to data processing for monitoring purposes at the workplace. It insists on the current regime being maintained, as to the circumstances under which employee monitoring can take place, or that employee monitoring be regulated by a strict CNPD regulation.

It is therefore unclear whether or not businesses will still have to require an authorisation for processing activities related to employee surveillance. It is likely that no prior CNPD authorisation will be required in the future but the staff delegation or, in the absence thereof, the employees can ask the CNPD for a prior opinion on the compliance of the monitoring system put in place. Equally, the general rules of the GDPR on the necessity to conduct a DPIA with a possible consultation of the CNPD may likely apply in such a case.

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

According to article L. 261-1 of the Labour Code, the consent of employees concerned does not necessarily render the processing lawful.

Information must be given to employees and staff delegation or in the absence thereof, the Labour and Mines Inspectorate (ITM). There are no substantial changes foreseen in the future legal framework.

In all cases, employees' rights under the GDPR must be respected, e.g., they must be fully informed of the monitoring put in place. A clear employee's privacy policy could be a way to provide notice to employees.

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

Under the current regime, staff delegation has a co-decision power for companies hiring more than 150 employees for processing under numbers 1, 4 and 5 (as laid down in article L. 261-1 of the Labour Code) regarding the establishment of data processing for supervisory purposes in the workplace.

The draft bill N°7184 provides that a staff delegation, or the employees concerned, could seek the prior opinion of the CNPD on the compliance of any monitoring project in the workplace, with suspensive effects and with the result that the CNPD will have to take position within a month. It is not yet clear whether such opinion is binding or not.

## **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 EUR 20 million or 4% of worldwide turnover, whichever is the highest.

## 16 Enforcement and Sanctions

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

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
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.	N/A
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).	N/A
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.	N/A
Imposition of Administrative Fines for Infringements of Specified GDPR Provisions	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.	N/A

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
Non-Compliance With a Data Protection Authority	The GDPR provides for administrative fines which will be EUR 20 million or up to 4% of the business' worldwide annual turnover of the proceeding financial year, whichever is higher.	N/A

### 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. According to the draft bill N°7184, the CNPD will indeed have such powers.

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

Considering the upcoming implementation of the GDPR, there are no recent cases as to the CNPD's approach of those powers.

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

Following the 2015 Schrems case, national authorities can exercise their powers against businesses established in other jurisdictions. Furthermore, according to the GDPR, European data protection authorities must cooperate and assist one another when necessary.

As an example, the CNPD approved the Binding Corporate Rules of a business established in Luxembourg, and other Member States, as well as in other non-European jurisdictions. Following the co-operation and mutual recognition procedure, all European data protection authorities then approved the results obtained by the CNPD.

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

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

There is no publicly available data on that matter.

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

The CNPD has not issued a guidance on e-discovery. However, it takes into account the 2009 WP29's working document on the information exchange procedure prior to trial in transnational civil proceedings (WP158).

## 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 that matter.



#### Véronique Hoffeld

Loyens & Loeff Luxembourg S.à r.l.  
18-20 rue Edward Steichen  
L-2540 Luxembourg  
Luxembourg

Tel: +352 466 230  
Email: [veronique.hoffeld@loyensloeff.com](mailto:veronique.hoffeld@loyensloeff.com)  
URL: [www.loyensloeff.com](http://www.loyensloeff.com)

Véronique Hoffeld is a member of the Management Committee of Loyens & Loeff Luxembourg and heads the Luxembourg Litigation & Risk Management Practice Group. She covers matters in the areas of commercial law (negotiation of contracts), litigation, arbitration and data protection.

She has experience in advising on a broad range of complex, high-value multi-jurisdictional litigations and arbitrations. She focuses in particular on commercial disputes especially financial and corporate litigation. Together with her team she has been rewarded by various high-profile arbitration cases that have involved interesting and partly unresolved issues related to the recognition and enforcement of ICC arbitral awards.

Prior to joining Loyens & Loeff Luxembourg, Véronique worked for more than 10 years in another important Luxembourg law firm, at which she was made partner in 2003.

Véronique has been a member of the Luxembourg Bar since 1996.

She is the president of the board of directors of the National Research Fund (FNR) of Luxembourg.

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

The finalisation and adoption of the draft bill N°7184.



#### Florence D'Ath

Loyens & Loeff Luxembourg S.à r.l.  
18-20 rue Edward Steichen  
L-2540 Luxembourg  
Luxembourg

Tel: +352 466 230  
Email: [florence.d.ath@loyensloeff.com](mailto:florence.d.ath@loyensloeff.com)  
URL: [www.loyensloeff.com](http://www.loyensloeff.com)

Florence D'Ath is a member of Loyens & Loeff's Litigation & Risk Management Practice Group in Luxembourg.

She advises clients on general commercial law and also represents them in court and in alternative dispute resolution proceedings. She also is a member of the Benelux Food & Beverages and Healthcare & Life Sciences Teams.

Florence specialises in general commercial law, intellectual property, regulatory (including in the Food and Health/Life Sciences sector) and ICT law (in particular in privacy and data protection).

She joined Loyens & Loeff in January 2015. Florence has been a member of the Brussels Bar since 2015.



Loyens & Loeff is a leading independent Luxembourg law firm which provides comprehensive and fully integrated legal and tax advice on corporate and commercial law, tax law, banking and finance, investment management, M&A, private equity, real estate and litigation. Our clients include private companies, family offices, financial institutions, investment funds and individuals.

The close cooperation between legal and tax specialists within a single firm places us in a unique position both in our home market, the Benelux and Switzerland, and internationally, and benefits our clients by facilitating an approach to issues from different angles, creating synergies and increasing efficiency.

Loyens & Loeff's culture is characterised by a strong sense of independence, entrepreneurship, high-quality services and involvement. The principles of quality, transparency and short-line communication form the foundation for an informal and inspiring culture, which stimulates the search for pragmatic but secure solutions to complex legal and tax issues. Loyens & Loeff pays particular attention to education and training, and to creating an exciting and challenging work environment. This enables the firm to attract outstanding young talent and to guarantee the highest standards of service.



# Macau

Pedro Cortés



Rato, Ling, Lei & Cortés – Advogados

José Filipe Salreta



## 1 Relevant Legislation and Competent Authorities

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

Law no. 8/2005, of August 22 – Personal Data Protection Act (“*Lei da Protecção de Dados Pessoais*” in Portuguese, or LPDP) of the Macau Special Administrative Region (henceforth “MSAR”).

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

The Chief Executive Dispatch no. 83/2007, of March 12, (and ancillary legislation) created the Office for Personal Data Protection (“*Gabinete de Protecção de Dados Pessoais*” in Portuguese, or “GPDP”).

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

Yes – Law no. 2/2012, of March 19, on the Legal Regime of video surveillance in public spaces (“*Regime jurídico da videovigilância em espaços públicos*” in Portuguese).

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

The GPDP is the entity responsible for the monitoring and coordination of compliance with the LPDP, as well as for the establishment of an adequate confidentiality regime and the monitoring of its execution.

## 2 Definitions

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

#### ■ “Personal Data”

“Personal Data” is defined as: “any information of any kind and regardless of the respective format, pertaining to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, namely by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity”.

#### ■ “Processing”

“[Data] Processing” is defined as “any operation or set of operations performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction”.

#### ■ “Controller”

The term “Controller” does not exist as such in the LPDP. The closest definition pertains to the “[entity] responsible for processing”, which is defined as “the natural or legal person, public authority, agency or any other body which alone or jointly with others, determines the purposes and means of the processing of personal data” (henceforth “data controller”).

#### ■ “Processor”

The term “Processor” also does not exist as such in the LPDP. The closest definition pertains to “subcontractor”, which is defined as “a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the data controller” (henceforth “data processor”).

#### ■ “Data Subject”

“Data Subject” is defined as “the individual person to which the data being processed pertains”.

#### ■ “Sensitive Personal Data”

“Sensitive Personal Data” is referred to in article 7 of the LPDP, which prohibits the processing of personal data concerning political or philosophical beliefs, political or trade-union membership, religious faith, private life, racial or ethnic origin, as well as the processing of data concerning health and sex life, including genetic information, with the exceptions foreseen by the LPDP.

#### ■ “Data Breach”

The term “Data Breach” does not exist as such in the LPDP – however, the law provides for the definition of wrongful or undue access as the unauthorised access to personal data by any entity who is not entitled to do so, and stipulates a penalty of imprisonment up to one year or a fine of up to 120 days (with the aggravating factors indicated in the law and unless a more severe penalty exists by special law).

#### ■ Other key definitions – please specify (e.g., “Pseudonymous Data”, “Direct Personal Data”, “Indirect Personal Data”)

Other definitions provided by the LPDP include:

■ “personal data file” (“file”) is defined as “any structured set of personal data which are accessible according to specific criteria, regardless of the form or type of their creation, storage and organisation”;

- “**third party**” is defined as “any natural or legal person, public authority, agency or any other body other than the data subject, the data controller, the subcontractor or the persons who, under the direct authority of the data controller or of the subcontractor, are authorised to process the data”;
- “**recipient**” is defined as “a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a legal stipulation or of a regulatory requirement of organic nature shall not be regarded as recipients”;
- “**data subject’s consent**” is defined as “any freely given specific and informed indication of his/her wishes by which the data subject signifies his agreement to personal data relating to him being processed”; and
- “**interconnection of data**” is defined as “data processing which consists in the possibility of correlating data in a file with the data in a file or files kept by another or other controllers, or kept by the same controller for other purposes”.

### 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 LPDP only provides a territorial scope for its applicability regarding video surveillance or other means of capturing, processing and disseminating sounds and images to identify persons whenever the controller is domiciled or domiciled in the MSAR, or uses a computer and telematic network access provider established therein.

Therefore, the LPDP shall apply in accordance to its material scope, i.e. it shall apply to the processing of personal data by means wholly or partly by automated means, as well as processing by non-automated means of personal data contained in or intended for manual files, regardless of the establishment of businesses in other jurisdictions.

Although the LPDP would *de jure* be applicable in the case above, the jurisdiction of the OPDP would *de facto* have implementation difficulties regarding a business established in another jurisdiction and with no presence in Macau.

### 4 Key Principles

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

- **Transparency**  
Data processing shall be made in a transparent way and in strict compliance with the respect of privacy (article 2 of the LPDP).
- **Lawful basis for processing**  
Data shall be processed in a lawful way and in compliance with the principle of good faith, as well as with the principles enunciated in article 2 of the LPDP, which include the respect of rights, freedoms and guarantees in the MSAR, in international instruments and in existing legislation (article 5, paragraph 1, subparagraph 1 of the LPDP).  
Article 6 of the LPDP further provides that the processing of personal data may only be carried out if the data subject has given his/her unequivocal consent, or if the processing is necessary for the:

- 1) execution of contracts or contracts in which the data subject is a party or prior to the formation of the contract or declaration of negotiation will be made at his request;
- 2) compliance with a legal obligation to which the controller is subject;
- 3) protection of vital interests of the data subject, if he/she is physically or legally incapable of giving his/her consent;
- 4) execution of a mission of public interest or in the exercise of powers of a public authority in which the controller (or a third party to whom the data are transmitted) is invested; and
- 5) pursuit of legitimate interests of the controller or third party to whom the data are transmitted, provided that the interests or rights, freedoms and guarantees of the data subject shall not prevail.

- **Purpose limitation**

Data shall be collected for specific, determined and lawful purposes, which are directly related to the activity of the data controller, and cannot subsequently be processed in a way that is incompatible with those purposes (article 5, paragraph 1, subparagraph 2 of the LPDP).

- **Data minimisation**

No specific stipulation – this principle is included in article 5, paragraph 1, subparagraph 3 of the LPDP (see “Proportionality” below).

- **Proportionality**

Data shall be adequate, pertinent and non-excessive in relation to the purposes for which they are collected and processed (article 5, paragraph 1, subparagraph 3 of the LPDP).

- **Retention**

Data shall be kept in a way which allows the identification of its owner only for the duration necessary for the purposes of collection or subsequent processing (article 5, paragraph 1, subparagraph 5 of the LPDP).

- **Other key principles – please specify**

The LPDP also stipulates that data shall be exact and, if necessary, shall be updated, with the obligation to ensure that inexact or incomplete data are erased or amended, in compliance with the purposes for which data was collected or subsequently processed (article 5, paragraph 1, subparagraph 5 of the LPDP).

### 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 LPDP guarantees the right of the data subject to information regarding the identity of the data controller or its representative, the purposes of processing and other ancillary information (article 10 of the LPDP), as well as the right of access to all his/her data (article 11 of the LPDP).

No specific provisions exist regarding the right to obtain a copy of the personal data.

- **Right to rectification of errors**

The right of access includes the right to rectify, delete or block data which processing does not comply with the LPDP, namely in regards to the incomplete or inexact character of those data (article 11, paragraph 1, subparagraph 4 of the LPDP).

- **Right to deletion/right to be forgotten**

See above regarding the right to deletion. Regarding the right to be forgotten, no specific provisions exist regarding such right. Please note, however, that under the LPDP, personal

data shall be kept in a way which allows the identification of its owner only for the duration necessary for the purposes of collection or subsequent processing (as per the principle of retention above).

#### ■ **Right to object to processing**

The data subject has the right to object at any time, under lawful and serious reasons relating to his/her specific case, that his/her data be the subject of processing, in which case, under justified objection, the processing shall not concern those data (article 12, paragraph 1 of the LPDP).

#### ■ **Right to restrict processing**

Without prejudice to the right to object to the processing indicated above, no specific provisions exist regarding the right to restrict processing of personal data. Hence, as long as the data subject presents lawful and serious reasons relating to his/her specific case, he/she shall have the right to restrict processing.

#### ■ **Right to data portability**

No specific provisions exist regarding the right to data portability.

#### ■ **Right to withdraw consent**

No specific provisions exist regarding the right to withdraw consent. However, we are of the view that this right falls under the provisions regarding the data subject's right to object to processing (as indicated above) and, therefore, the data subject may withdraw consent insofar as he/she presents lawful and serious reasons relating to his/her specific case to do so.

#### ■ **Right to object to marketing**

The data subject also has the right to object, on request and free of charge, to processing of personal data concerning him/her for direct marketing or any other form of commercial prospecting, and also has the right to be previously informed of any transfer of data to third parties for the purposes of direct marketing or usage for third parties, as well as the right to object, free of charge, to such transfer or usage (article 12, paragraph 2 of the LPDP).

#### ■ **Right to complain to the relevant data protection authority(ies)**

The LPDP provides for the possibility to submit a complaint to the GPDP, without prejudice to the possibility of resorting to administrative or jurisdictional means to guarantee the compliance with legal and regulatory provisions (article 28 of the LPDP).

#### ■ *Other key rights – please specify*

The LPDP also includes the right not to be subject to automated individual decisions (article 13 of the LPDP) and the right to an indemnity in cases of illegal processing of data or of any act infringing legal or regulatory provisions regarding data protection (article 14 of the LPDP).

## 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?**

Any data processing is subject to notification of the GPDP, to be made within eight days of the start of such processing by the data controller or by its representative (article 21, paragraph 1 of the LPDP).

If there is transfer of personal data to a destination outside the MSAR, the opinion of the GPDP must be sought to confirm if such destination ensures an adequate level of protection. However, the transfer of personal data to a legal system which does not ensure an adequate level of protection pursuant to the LPDP may be effected by means of notification to the public authority, if the data subject has given his/her unequivocal consent to the transfer, or if that transfer is necessary under the cases provided by law – i.e. it is necessary for the formation of a contract between the data subject and the data controller, for preliminary measures for the formation of said contract by request of the data subject, among others (article 19, paragraph 1 and article 20, paragraph 1 of the LPDP).

The processing of sensitive data or of data related to credit and solvency of its subjects, the interconnection of personal data and the usage of personal data for purposes which are not decisive to the collection of such data are subject to previous authorisation by the GPDP, without prejudice to legal or regulatory exceptions (article 22 of the LPDP).

### 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)?**

Any requests for authorisation, notification or opinion sent to the GPDP shall contain the information provided by law, in particular:

- 1) name and address of the data controller and, if applicable, its representative;
- 2) purpose of data processing;
- 3) description of the categories of data subjects and data or categories of personal data concerning said data subjects;
- 4) recipients or categories of recipients to whom the data may be disclosed and under which conditions;
- 5) entity in charge of the processing of data, if not the data controller;
- 6) possible interconnection of processing of personal data;
- 7) personal data storage period;
- 8) form and conditions for data subjects to have knowledge of or to amend their respective personal data;
- 9) expected data transfers to third countries or territories; and
- 10) general description enabling a preliminary assessment of the suitability of measures taken to ensure the adequate level of protection under the LPDP (in accordance with articles 15 and 16 of the LPDP).

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

As previously indicated, any data processing (see "[data] processing" definition above) is subject to notification of the GPDP, regardless of the entity responsible for the processing, without prejudice to the cases where previous consent of the GPDP must be sought.

### 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 data controller or its representative have the obligation to notify the GPDP, as per article 21, paragraph 1 of the LPDP.

**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)?**

Any requests for an opinion or authorisation, as well as notifications, sent to the GPDP shall contain the information indicated in subparagraph 2 above (article 23 of the LPDP).

In case of sensitive data processing (article 7, paragraph 2 of the LPDP), of the creation and maintenance of records regarding suspicions of illegal activities, criminal offences and administrative offences (article 8, paragraph 1 of the LPDP), and of requests for authorisation, as well as those pertaining to records of processing of personal data shall indicate, at least:

- 1) the person responsible for the file and, where appropriate, his representative;
- 2) the categories of personal data processed;
- 3) the purposes for which the data are intended and the categories of entities to whom it may be transmitted;
- 4) how the right of access and of rectification of data can be exercised;
- 5) possible interconnections of processing of personal data; and
- 6) expected data transfers to third countries or territories.

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

The lack of notification or authorisation request as provided by the LPDP entails a fine between 2,000 and 20,000 MOP for individuals and a fine between 10,000 and 100,000 MOP for legal persons. The fine shall be increased to twice its limits in the case of data subject to prior authorisation (in accordance with article 22 of the LPDP).

**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 (without prejudice to the obligation to notify the GPDP regarding any new data processing).

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

As indicated above, the processing of sensitive data or of data related to credit and solvency of its subjects, the interconnection of personal data and the usage of personal data for purposes which are not decisive to the collection of such data are subject to previous authorisation by the GPDP, without prejudice to legal or regulatory exceptions (article 22 of the LPDP).

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

The registration/notification is currently not possible online.

**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?**

No timeframe currently exists for the procedure of prior approval.

## 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 – such possibility is not previewed by the LPDP.

**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 to 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 – however, this information shall be included in the notification to be submitted by the applicant to the GPDP (see above).

**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 LPDP stipulates that, where processing is carried out on the data controller's behalf, said data controller must choose a processor providing sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out, and must ensure compliance with those measures.

The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that the processor shall act only on instructions from the controller, that the obligations incumbent on the data controller shall also be incumbent on the processor, *inter alia*:

- a) The data processor must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.
- b) The measures indicated above must ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected, according to the state of the art and the cost of their implementation.

### 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 carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that the processor shall act only on instructions from the controller, and that the obligations set out in paragraphs a) and b) above shall also be incumbent on the processor.

For the purposes of keeping proof, the parties of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in the previous question must be in writing in a document with legally recognised probative value.

## 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 indicated above, data shall be collected for specific, determined and lawful purposes, which are directly related to the activity of the data controller, and cannot subsequently be processed in a way that is incompatible with those purposes (article 5, paragraph 1, subparagraph 2 of the LPDP).

Also, as stated in question 4.1 above, the processing of personal data may only be carried out if the data subject has given his/her unequivocal consent, or if the processing is necessary to the cases referred to in article 6 of the LPDP.

Hence, if the processor has declared marketing communications (be it via electronic direct marketing or via other means) as one of the purposes of processing, and if the data subject has given his/her consent to such purpose, such processing is lawful under the LPDP.

### 9.2 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 answer above.

### 9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

See answer above. Also, regarding certain industries (e.g. banking and financial industries), the sending of marketing is specifically forbidden to prospective clients without the entity being duly licensed in the MSAR.

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

No available data.

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

No specific provisions exist regarding such purchase, although said purchase might constitute an unlawful transfer of personal data if the proper consent from the data subject has not been sought.

### 9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

If the measures indicated in question 9.1 have not been taken, the entity responsible for treatment is liable to an administrative offence, punishable with a fine between 8,000 and 80,000 MOP, for the non-compliance with the obligations under article 6 of the LPDP (article 33 of the LPDP).

## 10 Cookies

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

The LPDP does not specifically provide for the use of cookies – hence, opt-in consent must be sought with the data subject.

### 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?

This is not applicable.

### 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 transfer of personal data abroad can only take place under the stipulations of the LPDP and only if the legal order to which data are transferred ensures an adequate level of protection. Such level of protection is assessed by the GPDP on a case-by-case basis (article 19 of the LPDP).

### 11.2 Please describe the mechanisms companies 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 data abroad may be possible under the exceptions provided by the LPDP, which include the need of such transfer for the formation of a contract between the data subject and the data controller, and for preliminary measures for the formation of said contract by request of the data subject, among others.

However, the most common exception to the rule indicated above is the obtaining of the data subject's unequivocal consent to the transfer (article 20, paragraph 1 of the LPDP).

### 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 no list of legal orders ensuring an adequate level of protection currently exists, the transfer of personal data abroad is subject to previous authorisation by the GPDP, as indicated above. If unequivocal consent of the data subject is obtained, or if the situation under analysis falls under one of the exceptions provided by the LPDP, a simple notification is enough.

No timeframe currently exists for the procedure of assessment of the level of protection of a given legal order by the GPDP.

## 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.)?

No provisions exist in the LPDP regarding whistle-blower hotlines nor binding guidance issued by the GPDP. As indicated in question 5.1 above, the LPDP provides for the possibility to submit a complaint to the GPDP, without prejudice to the possibility of resorting to administrative or jurisdictional means to guarantee the compliance with legal and regulatory provisions (article 28 of the LPDP).

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

No provisions exist in the LPDP regarding this issue, and to the best of our knowledge, there is no binding guidance on this matter.

## 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 LPDP applies to video surveillance and to other means of capturing, processing and disseminating sounds and images to identify persons, whenever the controller is domiciled or headquartered in the MSAR, or uses a provider of access to computer and telematic networks established there (article 3, paragraph 3 of the LPDP).

No other specific stipulations exist for video surveillance, with the exception of Law no. 2/2012, of March 19, which establishes the legal framework of video surveillance in public spaces by the security forces and services of the MSAR.

As the use of CCTV is a separate processing of data, it shall require a separate notification to the GPDP under the law.

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

In accordance with GPDP guidelines, and without prejudice to the principles of purpose limitation and proportionality set out in question above, data controllers shall obey the following rules regarding CCTV in order not to violate the PDPA regime, as well as other stipulations contained in other legislation such as the Macau Penal Code:

- Only images can be recorded, not sound.
- The camera cannot be hidden and its existence must be publicised.
- The system cannot be connected to a public network (for instance, Wi-Fi networks or remote control functions).
- The areas covered by the footage should not be excessive, i.e. they should not include neighbouring areas.

- Security must be the exclusive purpose of data collection.
- Third parties cannot have access to the data, except when allowed by law.
- It is forbidden to replay recorded footage.
- The data can only be preserved for 6 (six) months.

## 14 Employee Monitoring

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

Without prejudice to the data which shall be mandatorily collected by the employer under the Macau Labour Law, no specific provision exists on this matter.

Therefore, employee monitoring is possible if it is necessary under the cases provided by the LPDP, or if consent has been sought.

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

Under the LPDP, the processing of data can only take place if the data subject has given his/her unequivocal consent to the transfer, or if that transfer is necessary under the cases provided by law (see “Key Principles” above).

As indicated above, the LPDP also allows for the processing of data if such processing is necessary for pursuing legitimate interests of the data controller or third party to whom the data are communicated, insofar as the interests or rights, freedoms and guarantees of the data subject do not prevail.

In the case of employee monitoring, the usual procedure to obtain consent would be to prepare an appropriate declaration of consent describing the applicable rules and rights of the data subject/employee under the LPDP.

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

No specific provisions exist on this matter.

## 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 – in accordance with the LPDP, the data controller shall implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction, accidental loss, unauthorised disclosure or access, *inter alia*, when processing involves transmission over a network, and against any form of unlawful processing, having regard to the available technical knowledge and to the costs resulting from its implementation, an adequate level of security with regard to the risks involved with the processing and the nature of the data to be protected (article 15, paragraph 1 of the LPDP).

The LPDP also provides for special security measures in case of sensitive data processing and of the creation and maintenance of records regarding suspicions of illegal activities, criminal offences and administrative offences (article 7, paragraph 2, article 8,

paragraph 1 and article 16, paragraph 1 of the LPDP), namely appropriate measures to:

- prevent unauthorised access to the premises used for the processing of such data (control of entry to the premises);
- prevent data carriers from being read, copied, altered or removed by an unauthorised person (control of data carriers);
- prevent unauthorised entry, as well as unauthorised disclosure, alteration or deletion of inserted personal data (insertion control);
- prevent automated data processing systems from being used by unauthorised persons through data transmission facilities (monitoring of use);
- ensure that authorised persons can only access the data covered by the authorisation (access control);
- ensure the verification of entities to whom personal data may be transmitted through data transmission facilities (transmission control);
- ensure that there is a *a posteriori* verification, within a period appropriate to the nature of the processing, to be laid down in the rules applicable to each sector, of the personal data to be introduced, when and by whom (introduction control); and
- prevent the data from being read, copied, altered or disposed of in an unauthorised manner during the transmission of personal data and in the transport of its medium (transport control).

Also, the LPDP requires that the systems must ensure the logical separation of data on health and sexual life, including genetic data, from other personal data (article 16, paragraphs 1 and 3 of the LPDP).

In case of sensitive data indicated in article 7 of the LPDP, the GPDP may require the encryption of data for transmissions over a network, if said transmission may imperil rights, freedoms and guarantees of the data subjects (article 16, paragraph 4 of the LPDP).

### 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) expects voluntary breach reporting.

No specific provision exists on this matter.

### 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) expects voluntary breach reporting.

Without prejudice to the right of information, which may be exercised by the data subject, no specific provision exists on this matter.

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

The non-compliance with the special security measures for sensitive data processing and for the creation and maintenance of records regarding suspicions of illegal activities, criminal offences and administrative offences, set out in article 16 of the LPDP and

described in question 15.1 above, is an administrative offence which may entail a fine between 4,000 and 40,000 MOP.

Although the LPDP provides penalties for undue access, as well as for tampering or the destruction of personal data, it does not specifically provide for security breaches by the data controller. It should be noted, however, that the LPDP mandates that the data controller shall present the notification/authorisation request with a general description of the security measures indicated in question 15.1 above, so that the GPDP may evaluate the adequacy of such measures. If the GPDP notifies the above-mentioned entity to address any insufficiency in the security measures and no remedy is taken, then a fine between 2,000 and 20,000 MOP for individuals and a fine between 10,000 and 100,000 MOP for legal persons may be imposed.

In case of wrongful or undue access to personal data by any entity who is not entitled to do so, the LPDP stipulates as maximum penalty two years of imprisonment or a fine of up to 240 days (unless a more severe penalty exists by special law).

## 16 Enforcement and Sanctions

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

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
Non-compliance with notification of data processing/compliance in breach of the terms set out in article 23 LPDP, providing false information, after notification by the GPDP and maintaining access to open data transmission networks for the data controllers which do not comply with the provisions of the LPDP.	A fine of between 2,000 and 20,000 MOP for individuals and a fine of between 10,000 and 100,000 MOP for legal persons; the fines are increased to twice the amount indicated above if the data are subject to previous authorisation.	
Non-compliance with stipulations of the LPDP regarding: 1) data quality (article 5); 2) right to information, access, objection, right not to be subject to automated individual decisions (articles 10 to 13); 3) special security measures (article 16); 4) processing by subcontractor (article 17); and 5) non-provision of mandatory information provided in article 24, paragraph 1.	A fine of between 4,000 and 40,000 MOP.	

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
Non-compliance with stipulations of the LPDP regarding: 1) conditions for legitimacy of data processing (article 6); 2) processing of sensitive data (article 7); 3) suspicions of illegal activities, criminal offences and administrative offences (article 8); 4) interconnection of personal data (article 9); and 5) transfer of data to a destination outside the MSAR and respective exemptions (articles 19 and 20).	A fine of between 8,000 and 80,000 MOP.	
Non-compliance with stipulations of the LPDP regarding: ■ purposefully omitting the notification/authorisation indicated in articles 21 and 22 of the LPDP; ■ providing false information in the notification/authorisation requests for the processing of personal data or making modifications in this request not allowed by the instrument of legalisation; ■ diverting or using personal data, in a manner incompatible with the purpose of the collection or with the instrument of legalisation; ■ promoting or carrying out an illegal interconnection of personal data; ■ non-compliance with the obligations provided for in this law or in other data protection legislation in the period established by the GPDP; and ■ maintaining access to open data transmission networks for those responsible for the processing of personal data that do not comply with the provisions of this law after notification of the GPDP not to do so.		Imprisonment of up to one year or a fine of up to 120 days.  The sanction is increased to twice the duration indicated above if the data involves sensitive data (article 7 of the LPDP) or suspicions of illegal activities, criminal offences and administrative offences (article 8 of the LPDP).



Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
<p>Access in any way to personal data whose access is forbidden to said individual/entity. The sanction is increased to twice the duration indicated when access:</p> <ul style="list-style-type: none"> <li>■ is achieved through violation of technical safety rules;</li> <li>■ has allowed the agent or third parties the obtainment of personal data; or</li> <li>■ has provided the agent or third parties with a benefit or patrimonial advantage.</li> </ul> <p>Deletion, destruction, damaging, suppression or modification of personal data without proper authorisation, rendering the data unusable or affecting their ability to be used.</p> <p>Qualified disobedience regarding notification to interrupt, cease or block the processing of personal data, or in cases of:</p> <ul style="list-style-type: none"> <li>■ refusal, without just cause, to cooperate as specifically requested by the GPDP;</li> <li>■ refusal to totally or partially destroy personal data; and/or</li> <li>■ refusal to destroy personal data, after the period of conservation provided for in the LPDP.</li> </ul>		<p>Imprisonment of up to one year or a fine of up to 120 days, unless otherwise provided by special law.</p> <p>The sanction is increased to twice the duration indicated in the cases provided.</p> <p>Imprisonment of up to two years or a fine of up to 240 days, unless otherwise provided by special law.</p> <p>The sanction is increased to twice the duration indicated if the damage resulting thereof is particularly serious.</p> <p>If the agent acts with negligence, the sanction is, in both cases provided above, imprisonment of up to one year or a fine of up to 120 days.</p> <p>Imprisonment of up to two years or a fine of up to 240 days.</p>

**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 GPDP, as the public authority referred to in LPDP (as well as in the article 79 of the Macau Civil Code), carries out the tasks conferred upon it and is (*inter alia*) responsible for the supervision and coordination of compliance with and enforcement of the LPDP, as well as for the establishment of the secrecy regime and supervision of its execution.

The GPDP is also responsible for encouraging and supporting the development of codes of conduct designed to contribute, depending on the characteristics of the different sectors, to the proper implementation of the provisions of the LPDP and, in general, to greater effectiveness of self-regulation and protection of fundamental rights related to the protection of privacy.

As no specific provision exists regarding the possibility of the GPDP issuing a ban on a particular processing activity, and without prejudice to the guidelines the GPDP may establish, we are of the view that such possibility is not within the powers of the public authority.

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

No available data.

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

No available data.

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

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

No available data.

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

No available data.

## 18 Trends and Developments

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

No available data.

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

No available data.

**Pedro Cortés**

Rato, Ling, Lei & Cortés – Advogados  
Avenida da Amizade  
555 – Macau Landmark Office Tower  
23<sup>rd</sup> Floor  
Macau

Tel: +853 2856 2322  
Email: [cortes@lektou.com](mailto:cortes@lektou.com)  
URL: [www.lektou.com](http://www.lektou.com)

Pedro Cortés has been a lawyer at Rato, Ling, Lei & Cortés – Advogados since 2003 and a partner since 2006, having extensive experience in gaming, corporate, finance and IP law.

Pedro has professional membership in the Macau Lawyers Association, the Portuguese Bar Association, the Brazilian Bar Association (São Paulo) the Hong Kong Institute of Directors, the International Association of Gaming Advisors (IAGA), the International Bar Association (IBA), the Chartered Institute of Arbitrators (CI Arb) and the Hong Kong Institute of Arbitrators (HKIA). He is also qualified to work as a lawyer in East Timor and is recognised by the Justice Department of Guangdong as a Cross-border Macau Lawyer.

Pedro has been a contributor for several legal and non-legal publications, including *China Outbound Investments*, *International Financial Law Review* and *International Law Office*.

**José Filipe Salreta**

Rato, Ling, Lei & Cortés – Advogados  
Avenida da Amizade  
555 – Macau Landmark Office Tower  
23<sup>rd</sup> Floor  
Macau

Tel: +853 2856 2322  
Email: [salreta@lektou.com](mailto:salreta@lektou.com)  
URL: [www.lektou.com](http://www.lektou.com)

José Filipe Salreta has been a lawyer at Rato, Ling, Lei & Cortés – Advogados since 2011. Previous to that, he was a Trainee Lawyer in the Portuguese law firm “SPS Advogados” between 2007 and 2009.

José is a member of the Macau Lawyers Association and the Portuguese Bar Association and works in commercial and corporate, labour, insurance, banking and litigation Law.

He has a Master's degree in European Studies from Sorbonne University, in France, and a Postgraduate degree in International Business Law from the University of Macau. José also contributes for several legal and non-legal publications.



Rato, Ling, Lei & Cortés – Advogados (Lektou) is a Macau SAR-based law firm with more than 30 years' experience of legal practice in Macau. Services regularly provided by the firm include issuing legal opinions and advising on Macau Law, helping international companies to start their businesses in Macau and assisting in the reorganisation of economic groups with connections to Macau.

In 2016, Lektou partnered with Zhong Yin Law Firm, in the People's Republic of China, and Fongs, in Hong Kong, to open a new office in Hengqin Island, Zhuhai, PRC – ZLF Law Firm. This is the first law office that unites firms from the two Special Administrative Regions and Mainland China. In 2017, Lektou opened an office in Lisbon, Portugal, as a part of its internationalisation strategy to position as a legal player in the platform between the PRC and Portuguese-speaking countries.

The academic and professional background, the update and specialisation, together with the experience of the lawyers of Lektou, are the key to answering the increasing demand of the firm's worldwide clients.

# Malta

GANADO Advocates

Dr. Paul Micallef Grimaud



Dr. Philip Mifsud



## 1 Relevant Legislation and Competent Authorities

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

From 25 May 2018, the principal data protection legislation in the EU will be Regulation (EU) 2016/679 (the “**General Data Protection Regulation**” or “**GDPR**”). The GDPR repeals Directive 95/46/EC (the “**Data Protection Directive**”) and leads to increased (though not total) harmonisation of data protection law across the EU Member States.

The provisions of the GDPR will be transposed directly into Data Protection Act (“**DPA**”), Chapter 440 of the Laws of Malta.

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

General legislation which currently impacts data protection includes:

- Notification and Fees (Data Protection Act) Regulations (Subsidiary Legislation 440.02).
- Third Country (Data Protection Act) Regulations (Subsidiary Legislation 440.03).
- Processing of Personal Data (Protection of Minors) Regulations (Subsidiary Legislation 440.04).
- Transfer of Personal Data to Third Countries Order (S.L. 440.07).

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

Current sector-specific legislation relating to data protection includes:

- Processing of Personal Data Electronic Communications Sector) Regulations (Subsidiary Legislation 440.01).
- Data Protection (Processing of Personal Data in the Police Sector) Regulations (Subsidiary Legislation 440.05).
- Processing of Personal Data (Police and Judicial Cooperation in Criminal Matters) Regulations (Subsidiary Legislation 440.06).
- Processing of Personal Data for the purposes of the General Elections Act and the Local Councils Act Regulations (Subsidiary Legislation 440.08).
- Processing of Personal Data (Education Sector) Regulations (Subsidiary Legislation 440.09).

Please note that these may be amended and/or repealed upon entry into force of the GDPR.

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

The relevant data protection regulatory authority is the Information and Data Protection Commissioner (“**IDPC**”).

## 2 Definitions

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

The definitions contained in the GDPR are expected to be adopted in the DPA and therefore, the following definitions are expected to appear in the DPA upon entry into force of the GDPR:

- “**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**” / “**Special categories of 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?

Maltese laws will not apply to businesses established in other Member States. However, where a business established outside the EU is processing data relating to individuals habitually resident in Malta, in accordance with the GDPR, these may be regulated by the Maltese data protection laws and fall under scrutiny of the IDPC.

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 interest are

overridden by the interests, fundamental rights or freedoms of the affected data subjects).

Businesses require stronger grounds to process sensitive personal data (special categories of 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; (iii) the processing is in the vital interest of the data subject or third parties where the data subject is incapable of providing consent; (iv) the data has been publicly revealed by the data subject; or (v) 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 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 is inaccurate is 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 appropriate security of that 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 for which the data is being processed; (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 was 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 is 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 is no longer needed for the original purpose (and no new lawful purpose exists); (ii) in the event that 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 has been processed unlawfully; or (v) erasure is necessary for compliance with EU law or national data protection law. This right is however limited in the cases expressly mentioned in Article 17(3) of the GDPR which are related, in the main, to public interest, the freedom of expression and information, legal obligations imposed on the controller to process the data, the exercising of official authority vested in the controller and the establishment, exercise or defence of legal claims.

#### ■ **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 the original purpose, but the data is 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 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 IDPC, if the data subjects live in Malta or the alleged infringement occurred in Malta.

#### ■ **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?

Currently, article 29 of the DPA provides that the controller shall notify the IDPC before carrying out any wholly or partially automated or manual processing operation. The IDPC shall maintain a register of processing obligations so notified. Notification is also required where there is a change in the processing activities that a controller conducts.

In accordance with the Third Country (Data Protection) Regulations (Subsidiary Legislation 440.03), data controllers must also notify the Commission prior to transferring personal data to a third country and obtain authorisation.

Other notification requirements include:

- notification by the data controller to the IDPC on the appointment or removal of a data representative (“PDR”); and
- notification by the data controller to the IDPC where the processing of personal data involves particular risks of improper interference with the rights and freedoms of the data subject.

The above notification obligations will no longer be applicable once the GDPR comes into force. This said, in accordance with the GDPR, the IDPC will need to be notified of the appointment of a Data Protection Officer (DPO) wherever this is required by the law. Other instances where the IDPC may need to be informed of data processing activities include those where the activities are deemed to be of high risk and not easily mitigated through technological means, as well as where third-country transfers are to rely on binding corporate rules.

### 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 to the IDPC, currently in place as referred to above, must specify:

- the name and address of the data controller and of any other person authorised by him in that regard, where applicable;
- the purpose(s) of the processing;
- a description of the category or categories of data subject and of the data or categories of data relating to them;
- the recipients or categories of recipients to whom the data might be disclosed;

- (e) proposed transfers of data to third countries; and
- (f) a general description allowing a preliminary assessment to be made of the adequacy of the measures taken to ensure the security of processing.

### 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 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)?

As the law currently stands, every controller of data must notify the IDPC where the DPA is applicable to them, e.g., where the controller is established in a third country but the equipment used for the processing of personal data is situated in Malta, a person established in Malta must be appointed to act as representative. In such a case, this representative is subject to the requirement of notification.

### 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 to the IDPC referred to above must specify:

- (a) the name and address of the data controller and of any other person authorised by him in that regard, where applicable;
- (b) the purpose(s) of the processing;
- (c) a description of the category or categories of data subject and of the data or categories of data relating to them;
- (d) the recipients or categories of recipients to whom the data might be disclosed;
- (e) proposed transfers of data to third countries; and
- (f) a general description allowing a preliminary assessment to be made of the adequacy of the measures taken to ensure the security of processing.

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

Currently, the failure to notify the IDPC of a processing operation prior to its commencement is punishable by an administrative fine of not less than €120 but not more than €600, and a daily fine of not less than €20 but not more than €60.

The failure to notify the IDPC of a processing obligation that involves risks of improper interference with the rights and freedoms of the data subject is subject to a fine of between €250 and €2,500 and a daily fine ranging from €25 to €250.

The failure to notify the IDPC of transfers of personal data to a third country is liable to an administrative fine not exceeding €23,293.73 for each violation and €2,329.37 for each day during which the violation persists.

This may change once the GDPR enters into force; however, guidance from the IDPC in this respect has not yet been made available.

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

Currently, a fee of €23.29 is payable upon the lodging of a notification in respect of the commencement of processing activities. In certain cases, there is an exemption from the payment of the fee. Upon entry into force of the GDPR, this will no longer be payable.

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

Annually. Upon entry into force of the GDPR, this will no longer be applicable.

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

Currently, prior approval from the IDPC is required for the processing of sensitive personal data for research and statistics purposes.

Approval is also required in the case of transfers of data to third countries.

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

No, registration/notification cannot be completed online.

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

Yes, however, one must physically attend the office of the IDPC or, alternatively send an email request for a registration form in respect of a particular entity.

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

Registration/notification usually takes two to three working days.

## 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.

### 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 to 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 (“DPIAs”) 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 details of the Data Protection Officer must be published although not necessarily 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”) recommends 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 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 obligations imposed on the controller in relation to the appointment of processors when, in turn, appointing 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 (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?)

The controller must inform the data subject of his right to object at no cost to the processing of his personal data for direct marketing purposes.

### 9.2 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.).

With respect to other means of marketing including unsolicited communications by automated calling machines, fax or email, the subscriber (both a natural or legal person) must give their prior consent to their personal data being used for direct marketing purposes. If email contact details were given by the subscriber in relation to the sale of a product or service, these may be used for direct marketing; however, customers must be given the opportunity to object free of charge and in an easy manner to such use of their details at the time of their collection, as well as on each message sent to the customer.

Direct marketing carried out through any other means of communication requires a free means to opt out of such communications.

### 9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

Yes, they do.

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

Yes, the IDPC has dealt with cases involving breaches of marketing restrictions.

### 9.5 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 entity making such marketing lists available should inform the data subject, on obtaining of consent to process personal data, that the list may be sold to third parties for the purposes of such third parties sending marketing communications and having the data subject signify specific consent in this respect.

Where the marketing list has been purchased, the purchaser should, when sending out marketing communications, indicate where the personal details were obtained from, together with the other information listed in article 14 of the GDPR.

### 9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

Currently, the sending of marketing communications over automated calling machine, fax or email in breach of applicable restrictions is punishable by an administrative fine not exceeding €23,293.73 for each violation and €2,329.37 for each day during which such violation persists.

## 10 Cookies

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

Currently, Malta 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 Directive 95/46/EC and, from 25 May 2018, the GDPR). For consent to be valid, it must be informed, specific, freely given and must constitute a real 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, which means that it must be essential to fulfil their request.

### 10.2 The EU Commission intends to pass a new ePrivacy Regulation that will replace the respective national legislation in the EU Member States. The regulation is planned to come into force May 25, 2018 and will provide amended requirements for the usage of cookies. Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

Currently, there is no distinction as regards different types of cookies.

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

To our knowledge, the IDPC has not taken any enforcement action in relation to cookies as yet.

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

Currently, breaches of applicable cookie restrictions are punishable by an administrative fine not exceeding €23,293.73 for each violation and €2,329.37 for each day during which such violation persists.

## 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) or the business has implemented one of the required safeguards as specified by the GDPR.

### 11.2 Please describe the mechanisms companies 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 data exporter) and a processor (as data 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.

Transfer of personal data to the US is also possible if the data importer has signed up to the EU-US Privacy Shield Framework, which was designed by the US Department of Commerce and the EU Commission to provide businesses in the EU and the US with a mechanism to comply with data protection requirements when transferring personal data from the EU to the US.

### 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.

Currently, transfers of data to third countries require approval from the Commissioner who determines whether the country ensures an adequate level of protection. This must be notified to the IDPC by means of the following International Data Transfer form: <http://idpc.gov.mt/en/Documents/International%20Data%20Transfer%20Form.pdf>.

If the data is transferred to a third country which does not ensure an adequate level of protection on any of the grounds contained in Article 28(2) of the DPA (outlined in the answer to question 8.1 above), such a transfer must also be authorised to the IDPC.

As regards Standard Contractual Clauses and Binding Corporate Rules, these must also be submitted to the IDPC for review.

There are no time limits established for these approval or notification procedures, however, they do not usually exceed one week.

Upon entry into force of the GDPR, 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.

## 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 Protection of the Whistleblower Act, (herein the “PWA”) (Chapter 527 of the Laws of Malta) provides protection to employees in both the private sector and public administration to disclose information regarding improper practices.

The term “employee” is defined as:

- (a) a person who has entered into or works under a contract of service with an employer and includes a contractor or subcontractor who performs work or supplies a service or undertakes to perform any work or to supply services;

- (b) any person who has undertaken personally to execute any work or service for, and under the immediate direction and control of another person, including an outworker, but excluding work or service performed in a professional capacity to which an obligation of professional secrecy applies when such work or service is not regulated by a specific contract of service;
- (c) any person in employment in the public administration;
- (d) any former employee;
- (e) any person who is or was seconded to an employer;
- (f) any volunteer in terms of law; and
- (g) any candidate for employment, but only where information concerning a serious threat to the public interest constituting an improper practice has been acquired during the recruitment process or at another pre-contractual negotiating stage.

The scope of a report made in terms of the PWA is “improper practice”. This term includes an action or series of actions whereby:

- (a) a person has failed, is failing or is likely to fail to comply with any law and/or legal obligation to which he is subject;
- (b) the health or safety of any individual has been, is being or is likely to be endangered;
- (c) the environment has been, is being or is likely to be damaged;
- (d) a corrupt practice has occurred or is likely to occur or to have occurred;
- (e) a criminal offence has been committed, is being committed or is likely to be committed;
- (f) a miscarriage of justice has occurred, is occurring or is likely to occur;
- (g) bribery occurred, is occurring or is likely to occur;
- (h) a person is acting above his authority; or
- (i) information tending to show any matter falling within any one of the preceding paragraphs has been, is being or is likely to be deliberately concealed.

The provisions of the PWA do not apply to members of a disciplined force, members of the Secret Service or persons employed in the foreign, consular or diplomatic service of the Government.

One should also take note of the WP29 Opinion 1/2006 on the application of EU data protection rules to internal whistle-blowing schemes. This is limited 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. The WP29 recommends 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, or strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

No, it is not prohibited. However, anonymous reporting is not protected in terms of the PWA. Such an anonymous report may still be taken into account to determine whether an improper practice has occurred. If upon consideration of all circumstances, the report is deemed to be defamatory or libellous, it shall be discarded.

Additionally, anonymous reporting is not prohibited under the GDPR; however, it raises problems as regards the essential requirement that personal data should only be collected fairly. As

a rule, the WP29 considers 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)?

Yes, the data controller must notify the IDPC prior to physically installing CCTV cameras.

Furthermore, a 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.

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

The use of surveillance cameras must have a clearly defined specific purpose which is proportionate to the rights to privacy of individuals. The IDPC has also issued guidelines as to the use of biometric equipment at the workplace, establishing that this is only permissible in places demanding a high level of security and strict identification procedures.

## 14 Employee Monitoring

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

Please refer to question 14.2.

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

Individuals have the right to be informed about the processing of their personal data by means of a surveillance camera. The general practice is to provide the information by way of notices affixed in prominent and easily visible places within the monitored area. In certain cases, notices are also required to be affixed even before approaching the monitored area. The notice should include the designation of the data controller, the purpose for processing and a clear sign indicating the camera.

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

As regards biometric scanning, the IDPC establishes that where employees are unionised, there should be prior and proper consultation with the respective union.

## 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.

Upon entry into force of the GDPR, the controller will be 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?**

Currently, the maximum administrative penalty that may be imposed is €23,300. Upon entry into force of the GDPR, the maximum penalty will be increased to the higher of €20 million or 4% of worldwide turnover, depending on the nature of the breach.

## 16 Enforcement and Sanctions

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

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
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.	N/A
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).	N/A

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
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.	N/A
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.	N/A
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.	N/A

**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 IDPC carries out all these powers, in particular on-site inspections. (Please note that the Office of the IDPC has not issued Annual Reports since 2011 and recent information is limited.)

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

To our knowledge, the IDPC has not exercised its powers against businesses established in other jurisdictions.

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

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

Transfers of personal data in the context of police and judicial cooperation may only take place upon a request submitted in writing to the body exercising police powers. Such a request shall include an indication of the person or body making the request and of the reason and purpose for which the request is made. The communication of personal data must follow the principles of good data processing referred to in the answer to question 4.1 above.

The Data Protection (Processing of Personal Data in the Police Sector) Regulations provide that such transfers of data may only be made if there exists a legal obligation to do so or the communication is necessary for the prevention of a serious and imminent danger, or is necessary for the suppression of a serious criminal offence.

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

The IDPC has not issued any guidance on this point.

## 18 Trends and Developments

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

None with respect to the IDPC.



#### Dr. Paul Micallef Grimaud

GANADO Advocates  
171 Old Bakery Street  
Valletta VLT 1455  
Malta

Tel: +356 2123 5406  
Email: [pmgrimaud@ganadoadvocates.com](mailto:pmgrimaud@ganadoadvocates.com)  
URL: [www.ganadoadvocates.com](http://www.ganadoadvocates.com)

Dr. Paul Micallef Grimaud is the Partner heading the IP, Media, Entertainment and Technology practice group at GANADO Advocates. Paul's focus is dedicated to counselling and assisting clients in the drafting and negotiation of contracts, content and end-user related matters, the registration, protection and enforcement of IP rights, and competition and passing off disputes. Paul also leads the firm's practice related to the GDPR and regularly advises the firm's clients in relation to their data protection and privacy obligations, in light of the new regulations coming into force in 2018.



#### Dr. Philip Mifsud

GANADO Advocates  
171 Old Bakery Street  
Valletta VLT 1455  
Malta

Tel: +356 2123 5406  
Email: [pmifsud@ganadoadvocates.com](mailto:pmifsud@ganadoadvocates.com)  
URL: [www.ganadoadvocates.com](http://www.ganadoadvocates.com)

Dr. Philip Mifsud is an Associate within GANADO Advocates' Corporate Department, who regularly assists clients in all corporate matters including advice on governance matters, assistance with financing, M&A transactions, voluntary dissolutions and various other transactional projects. Philip also works in the IP, Media, Entertainment and Technology practice area, which incorporates data protection, and gives advice on matters such as the registration of trademarks, copyright law, review of franchising agreements, and the drafting and review of software licences. Philip works closely together with Dr. Paul Micallef Grimaud on advising clients on their obligations resulting from the GDPR.

## GANADO ADVOCATES

GANADO Advocates is a leading commercial law firm with a particular focus on the corporate, financial services and maritime sectors, predominantly servicing international clients doing business in or out of Malta. The firm traces its roots back to the early 1900s, and is today one of Malta's foremost law practices, consistently ranking as a leading firm in all its core sectors. GANADO Advocates has over the past decades contributed directly towards creating and enhancing Malta's hard-won reputation as a reliable and effective international centre for financial and maritime services. Today, the firm continues to provide high standards of legal advisory services to support and enhance Malta's offering.

The services offered by the IP, Media, Entertainment and Technology practice include data protection, the registration of trademarks, advice on and drafting of IP agreements, and representing clients in IP infringement lawsuits. The firm leads a project for the Government of Malta bringing together the various Malta-based legal and advisory service providers with a view to overhauling the current IP legal framework and providing solid and innovative legislative solutions to the IP industries, not least involving blockchain and digital currencies.



# Mexico

Abraham Diaz



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 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. General regulations such as the Privacy Notice Rules, published in January 2013, and the Binding Self-Regulation Parameters, also published in January 2013. Please be advised that Mexican data protection laws and general legislations follow international correlative laws, directives and statutes, and thus have similar principles, regulation scope and provisions.

Moreover, there are other laws such as the Criminal Code, the Law for the Regulation of Credit Information Companies, provisions set forth in the Copyright Law, General Law for the Protection of Personal Data in the possession of Obligated Subjects, the Federal Consumers Law and some specific provisions set forth in the Civil Code and the Commerce Code.

### 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 implies 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 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, transfer or disposal of personal data.
- **“Controller”**  
Individual or private legal entity that determines the treatment of personal data.
- **“Processor”**  
The individual or legal entity that solely or jointly with another processes personal data on behalf of the Controller.
- **“Data Subject”**  
An identified or identifiable natural person.
- **“Sensitive Personal Data”**  
Personal data which concerns the private life of an individual, or the misuse of such information which may lead to discrimination or carry a serious risk to the individual. In particular, sensitive personal data is considered those that may reveal information such as ethnical or racial origin, 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 which occurred in any phase of the data collection, storage or use, which may affect in a significant manner the patrimonial or moral rights of individuals.

- *Other key definitions – please specify (e.g., “Pseudonymous Data”, “Direct Personal Data”, “Indirect Personal Data”)*
  - **“ARCO rights”**  
Refers to the access, rectification, cancellation or opposition rights to the personal data processing.
  - **“Consent”**  
Expression of will made by the data owner concerning data collection.
  - **“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 in 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 others, about: the terms for the collection of personal data; the identity of the Controller; the purpose of the data collection; the possible transfers of data; and the mechanisms for enforcing the ARCO rights.
  - **“Transfer”**  
Any data communication made to a different person other than the Collector or the Processor.

### 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 located out of Mexico will be subject to the terms of the Privacy Notice, and to the Law, only when the data controller transfers personal data collected in Mexico, in accordance with the provisions of the Law.

### 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 also makes clear that personal data can in no way be collected, stored or used through deceitful or fraudulent means.
- **Lawful basis for processing**  
The Collector 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 processed for the compliance of 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 processed in a clear, objective manner, not giving room for confusion.
- **Data minimisation**  
The Collector will be responsible and shall endeavour to make reasonable efforts so that the personal data processed are of the minimum necessary, according to the purpose that originated the collection of PI.

#### ■ **Proportionality**

Data controllers can only collect personal data that is necessary, appropriate and relevant for the purpose(s) of the collection.

#### ■ **Retention**

This translates into the obligation of the Collector to retain personal data only for the period of time necessary for complying with the purpose(s) for which the data was collected, with the obligation to block, cancel and suppress the personal data afterwards.

#### ■ *Other key principles – please specify*

##### ■ **“Responsibility”**

The Collector must safeguard and be accountable of 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 for this effect.

##### ■ **“Quality”**

This principle is accomplished when 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, in advance, with the aim of processing any PI.

##### ■ **“Loyalty”**

This consists of the obligation of the data 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 data controller at any time they request.
- **Right to rectification of errors**  
Data subjects have the right to request the rectification of any of its personal data held by a data controller, if it is inaccurate, incomplete or dated.
- **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 data controller may keep such personal data exclusively for the purposes of the responsibilities regarding the treatment. Likewise, the Law establishes some cases where the data controller is not obliged to cancel or delete the personal data.
- **Right to object to processing**  
Data owners have the right to object to the processing of their personal data due to a legitimate reason.
- **Right to restrict processing**  
Data owners have the right to restrict the processing of their personal data due to a legitimate reason.
- **Right to data portability**  
This right is not recognised yet in Mexican legislation on PI.

## ■ Right to withdraw consent

At any time, the data owner may withdraw his/her consent for the treatment of their personal data, for which the data controller must establish simple and free mechanisms, which allows 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, the data owners 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 owners 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 owner has been communicated by the data controller.

## ■ Other key rights – please specify

Right for a verification procedure. Data subjects will have the right to request before the data protection authority (DPA), a verification procedure, in which the authority will check the data 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.

Yes, 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?

The failure in appointing the Data Protection Officer (person or department) is not expressly regulated as an infringement yet.

### 7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect to 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, they 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 or department at least with the following qualifications: i) data privacy expertise; and ii) enough authority and resources to implement measures in order to protect the personal data.

#### 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 the 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?

No, it is not mandatory to appoint a Data Protection Officer, being only necessary to mention in the Privacy Notice the name and domicile of the person or department which 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 for 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 the agreements between the business and the Processor related to the treatment of the 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 regulation dealing with unsolicited text messages or spam emails, but the Federal Bureau for Consumer Protection operates a call blocking registry, called REPEP, covering both landlines and mobile phone numbers, which gives suppliers 30 days to stop making marketing calls, sending marketing messages and to stop disturbing the consumer at his/her registered address, electronic address, or by any other means.

#### 9.2 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.

#### 9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

Please refer to question 9.1 above.

#### 9.4 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.

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

Yes, but in the Privacy Notice the Controller must provide detailed information as to the data transfers that it is willing to make, involving PI, expressly indicating the name of the data processor(s), of the type, category of activity sector of the latter; and expressly indicating the purpose(s) of such transfer(s). Also, when required, a clause indicating whether or not the data subject consents to the data transfer.

#### 9.6 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\$1,317,141.34 (approximately US\$70,000).

## 10 Cookies

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

Yes. The Guidelines for elaborating the Privacy Notice require that individuals are informed as to any technology that allows the automatic collection of PI simultaneously to the first contact with the individuals; requiring data owners to request the consent from individuals through an opt-in mechanism, and informing individuals 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 have 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 fines of up to US\$680,000, and if the infringement persists, additional fines of up to US\$1,300,000 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 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 FLPPPIPE the consent will not be necessary only in the following cases:

- i) when expressly allowed by the Law;
- ii) when PI is available in public access sources;
- iii) when personal data has been dissociated;
- iv) when the collection of personal data is needed for the compliance of obligations derived of 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 companies 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 FLPPPIPE, 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 exactly in the same terms as the Controller.

### 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.

## 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 set 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, or strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do companies 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?

Mexican legislation is silent as to the types of employee monitoring that are permitted and the circumstances under which said monitoring is allowed.

Therefore, the balance as to the monitoring that can be made by employers and the respect to the privacy of employees has to be found in the general rules set forth in Article 16 of the Mexican Constitution, which regulates the right to privacy, and the general rules established by the legislation on Data Privacy. These rules should be interpreted by the Mexican Courts on a case-by-case basis, in order to generate jurisprudence in this regard.

For instance, video surveillance of public spaces at workplaces is allowed, while surveillance at restrooms and locker rooms is prohibited.

Monitoring phone calls made by employees is allowed, but only to determine the user of the phone call and the length of the call, and not the content of the call.

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

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 as a collection of PI, employers would be required to give employees notice as to the use of video surveillance technology at workplaces.

The Mexican DPA has elaborated a model short Privacy Notice to be used by any individual or company introducing video surveillance technology at their premises.

Said summary Privacy Notice must be visible at the entrance of the 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?

Employee representatives at councils/trade unions do not need to be either consulted or 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.)?

Article 19 of the Federal Law for the Protection of Personal Information in Possession of Private Entities requires every data controller to implement and maintain administrative, technical and physical security measures, which prevent 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, and for its implementation the data owner must consider the existing risk and the possible consequences for the data subjects, the sensitivity of the data and the technological development.

### 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) expects voluntary breach reporting.

There is no legal requirement to report data breaches to the Mexican DPA, and so far there are no guidelines for voluntary breach reporting to the Mexican DPA.

### 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) expects voluntary breach reporting.

If any phase of the data collection, storage or use 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.

Likewise, Article 64 of the Regulations of the FLPPPE 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 inform 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 for getting more information regarding the breach.

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

According to the Federal Consumers Protection Law, the penalties for data security breaches regarding marketing matters range from MXN\$260.56 to MXN\$833,823.71.

On the other hand, the Mexican DPA (INAI) is entitled to impose administrative sanctions such as fines of up to MXN\$25,000,000 (approximately USD\$1,400,000).

Additionally, there are two activities deemed as felonies related to the wrong use of PI, which are:

- i) When a data owner authorised to collect, store and use PI with the aim of profiting, causes a security breach in the database containing PI under its custody. This is sanctioned with imprisonment from three months and up to three years.
- ii) To collect, use or store PI, with the aim of profiting, through error or deceit of the data subject, or error or deceit of the person who has to authorise the transfer. This is sanctioned with imprisonment from six months and up to five years.

## 16 Enforcement and Sanctions

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

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
<p>The Mexican DPA (INAI) is entitled to conduct visits of inspection <i>ex officio</i> to any company, in order to determine the compliance to the legislation on PI.</p> <p>The INAI is also entitled to prosecute and resolve any complaint tending to enforce the ARCO rights of any individual.</p>	<p>The Mexican DPA is not entitled to declare damages, thus it is necessary to file an independent civil action before the Mexican Civil Courts for that effect.</p>	<p>As stated above, the FLPPPIPE provides some criminal sanctions if there is an intention to profit out of the security breach of PI.</p> <p>However, the Mexican DPA is not entitled to prosecute criminal actions, thus it is necessary to file the corresponding criminal complaint before the Attorney's General Office, and the criminal action will be decided by a Criminal Court.</p>
	<p>The administrative infringements set forth in the FLPPPIPE are prosecuted before the INAI, and the ruling that this DPA issues can further be appealed before the Federal Court for Administrative Affairs. The decision that this Court gets to issue can further be appealed through a constitutional rights action, known as Amparo, before the Federal Circuit Courts.</p>	

### 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 recognised in the Law in favour of the INAI. However, considering that the FLPPPIPE 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 Mexican Federal Administrative Courts.

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

So far there are no recent cases or precedents illustrating this authority.

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

Please refer to question 16.1 above.

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

### 17.1 How do companies 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, so that they can 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 Mexican DPA.

## 18 Trends and Developments

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

There are no trends which have emerged during the previous 12 months.

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

Last year, some amendments to the FLPPPIPE introduced the possibility for data controllers to adopt self-regulatory schemes, which if validated or certified by any entity approved by the Mexican DPA, will have the effect of a less strict treatment by the DPA, in case of any data breach event.

**Abraham Diaz**

OLIVARES  
Pedro Luis Ogazón 17  
San Ángel, 01000  
Mexico City  
Mexico

Tel: +52 55 5322 3000  
Email: [abraham.diaz@olivares.mx](mailto:abraham.diaz@olivares.mx)  
URL: [www.olivares.mx](http://www.olivares.mx)

Abraham Diaz co-chairs the Privacy and IT Industry group and has a wealth of knowledge across the IP spectrum. Abraham focuses his practice on copyright, trademarks and unfair competition, litigation, licensing and prosecution matters. He counsels clients on any IP-related matters, and handles matters involving trademarks, trade dress, product configuration, unfair competition, advertisement-related matters, false advertising, trade secrets, plant breeders' rights, vegetal varieties and Internet-related IP issues. His Internet experience includes handling domain disputes under the UDRP, as well as counselling clients concerning the development of websites and the protection of the content thereof.

He also counsels clients with regards to the correct implementation, monitoring and auditing of privacy management programmes, and crisis and data breaches management.

Because of his broad background, Mr. Diaz is perfectly placed to advise clients over a range of subject matters and can look at legal needs in this sector in a 360° way.

**Gustavo Alcocer**

OLIVARES  
Pedro Luis Ogazón 17  
San Ángel, 01000  
Mexico City  
Mexico

Tel: +52 55 5322 3000  
Email: [gustavo.alcocer@olivares.mx](mailto:gustavo.alcocer@olivares.mx)  
URL: [www.olivares.mx](http://www.olivares.mx)

Gustavo Alcocer joined OLIVARES as a Partner in 1999. He manages the Corporate and Commercial Law Group and is Co-Chair of the Life Sciences and Pharmaceuticals Group. Prior to joining OLIVARES, he acted as In-House Counsel for Banamex for 11 years in various positions, including Vice-President of International Legal Affairs in New York and Executive Vice-President and Assistant General Counsel for Grupo Financiero Banamex in Mexico City.

Mr. Alcocer possesses a wealth of transactional experience in M&A, finance and business law and advises our clients on complex M&A, finance, asset sale and acquisition, licensing, franchising, real estate transactional work and regulatory work. Clients routinely turn to him for sophisticated strategic advice regarding structuring, maintaining and expanding operations in Mexico and IP valuation and monetisation. Additionally, Mr. Alcocer has worked with international companies in FCPA and anti-bribery compliance, as well as privacy and personal data protection.



OLIVARES

OLIVARES' Data Privacy and Data Security team is well-versed not only in data protection and data security in Mexico, but also in the data protection models found in many other countries around the world.

This understanding of regulations governing data privacy and data security in Europe and major nations like the USA, allows our team to provide a comprehensive assessment of the obligations that must be fulfilled by companies wanting to expand their e-commerce activities into Mexico and Latin America.

Likewise, a concrete understanding of Privacy by Design allows our team to give professional advice for privacy impact assessment, audits, training, data breach detection, incident management and data breach notifications.

# Netherlands

Kim Lucassen



Loyens &amp; Loeff N.V.

Iram Velji



## 1 Relevant Legislation and Competent Authorities

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

From 25 May 2018 onwards, the principal data protection legislation in the EU will be Regulation (EU) 2016/679 (the “**General Data Protection Regulation**” or “**GDPR**”). The GDPR repeals Directive 95/46/EC (the “**Data Protection Directive**”) and leads to increased (though not total) harmonisation of data protection law across the EU Member States.

The GDPR allows Member States to derogate from the GDPR in their own national legislation on certain points. In the Netherlands, the national derogations have been established in the GDPR Implementation Act (*Uitvoeringswet Algemene Verordening Gegevensbescherming*, “**UAVG**”).

Upon the adoption of the UAVG, which the Senate (*Eerste Kamer*) has announced will be prior to 25 May 2018, the Dutch Data Protection Act (*Wet bescherming persoonsgegevens*, “**Wbp**”) will become void.

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

In the Netherlands, the Dutch Telecommunication Act (*Telecommunicatiewet*, “**DTA**”) implements certain requirements that are set out in Directive 2002/58/EC (as amended by Directive 2009/136/EC) (the “**ePrivacy Directive**”). For instance, legal restrictions with regard to the use of cookies and direct marketing can be found in article 11.7 of the DTA.

In January 2017, the European Commission published a proposal for an ePrivacy Regulation that would harmonise the applicable rules across the EU.

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

In the Netherlands, there are three sector-specific legislations which – in addition to the GDPR and UAVG – impact data protection legislation. These are:

1. The Police Data Act (*Wet politiegegevens*). This act regulates the processing of personal data carried out by the National Police, the special investigative bodies, the Royal Marshalls (*Marechaussee*) and the National Department of Criminal Investigation. It also applies to the tasks that the police carry

out for judiciary purposes (e.g. executing the Aliens Act (*Vreemdelingenwet*)).

2. The Basic Registration of Persons Act (*Wet basisregistratie personen*, “**WBP**”). In the Netherlands, personal data of all individuals residing in the Netherlands are registered in the basic registration (*basisregistratie personen*, “**BRP**”). The WBP regulates the correct use of the registered personal data, for instance by the municipalities.
3. The Judicial Information and Criminal Records Act (*Wet justitiële en strafvorderlijke gegevens*) regulates the processing of judicial data in personal files (obtained during an investigation, for instance), criminal records and the certificate of good behaviour (*verklaring omtrent het gedrag*).

In addition to the above, the intelligence and security act (*Wet op de inlichtingen- en veiligheidsdiensten*, “**Wiv**”), better known as the ‘*Sleepwet*’, which translates to English as the ‘trawling law’, extends the powers of the Dutch general safety and intelligence agency and of the military intelligence and safety agency allowing them to, *inter alia*, install wire taps targeting an entire geographic region or avenue of communication and to share it with allied spy agencies.

Moreover, various health care legislation provide for additional requirements concerning the processing of personal data within the context of health care. This includes the Medical Treatment Contracts Act (*Wet op de Geneeskundige Behandelingsovereenkomst*, “**WGBO**”) and the Supplementary Provisions for the Processing of Personal Data in Health Care Act (*Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg*).

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

Article 28 of the European Privacy Directive 95/46/EC explicitly provides for the existence of a supervisory authority, who shall act with complete independence in exercising the functions entrusted to it. In the Netherlands, this supervisory authority is the Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*, “**AP**”).

## 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 (“**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”** 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; 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”** 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 identified or identifiable natural person 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 for the purpose of uniquely identifying a natural person.
- **“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”)*
  - **“Consent”** means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

### 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 as a processor, 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 as a processor) process personal data of data subjects who are in the Union in relation to: (i) the offering of goods or services (whether or not in return for payment) to persons in the EU; or (ii) the monitoring of the behaviour of persons in the EU (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 or by a third party, except where such an interest is overridden by the interests, fundamental rights or freedoms of the affected data subject, in particular where the data subject is a child).

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 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

The processing must strike a balance between the means used and the intended aim in order to be a targeted and proportionate way of achieving the purpose. The processing is not proportionate if the purpose can be achieved by a less intrusive approach.

#### ■ 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.



■ *Other key principles – please specify*

**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.

**Integrity and confidentiality**

Personal data shall be processed in a manner that ensures appropriate security of the personal 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 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 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 AP if the data subject lives in, or the alleged infringement occurred in, the Netherlands.

■ *Other key rights – please specify*

**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?

Following the entry into force of the GDPR, there will no longer be a legal obligation for businesses to register with or notify the data protection authority (or any other governmental body) in respect of its 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)?**

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 only mandatory if this concerns government bodies and other public organisations and in circumstances where the processing includes (i) large-scale regular and systematic monitoring of individuals, or (ii) large-scale processing of sensitive personal data.

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 a wide range of sanctions (including penalties) as available under the GDPR.

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

The appointed DPO should not be dismissed or penalised for performing their tasks. The DPO is legally protected by the GDPR against unfair termination or unfair dismissal.

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

It is permitted to appoint one DPO by a group of undertakings, provided that the DPO is easily accessible from each of the establishments.

**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 relevant 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 of a 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 (“DPIAs”) 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. The UAVG does not provide for additional responsibilities.

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

In the Netherlands, each DPO (including voluntary DPOs) has to be registered with the AP using the online DPO registration form that the AP published on its website on 3 April 2018. Registrations of DPOs based on an earlier version of the form will become void following 25 May 2018.

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

The contact details of the DPO must be clearly communicated to the AP and to data subjects, for instance in a 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 business that appoints a processor to process personal data on its behalf is required to enter into an agreement with the processor. This agreement should, amongst other things, set 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).

#### **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 which sets out the elements mentioned under Article 28 paragraph 3 of the GDPR. 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 notifying a data breach and assists in obtaining approval from the 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 the 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?)**

Under Dutch law, the processing of personal data for the purpose of electronic direct marketing is subject to the GDPR and to the DTA. This means that the processing of personal data for direct marketing purposes requires a lawful basis according to article 6 GDPR. Generally speaking, article 6(1)(f) GDPR provides that required lawful basis for recital 47 regards direct marketing as a ‘legitimate interest’.

Notwithstanding the foregoing, the right of data subjects to object to data processing for the purposes of direct marketing remains unimpaired (article 21(2) and recital 70 GDPR).

In addition to these GDPR restrictions, article 11.7 DTA (*cf.* article 13 e-Privacy Directive) lays down further restrictions for certain types of direct marketing, or as it is called in the DTA: “unsolicited communication for commercial, idealistic or charitable purposes”. Article 11.7(1) DTA bans electronic direct marketing without prior consent of the recipient using the publicly available electronic communications service. The sender of unsolicited communications must therefore be able to demonstrate the prior consent.

Under certain conditions, however, article 11.7(2) DTA alleviates the foregoing restriction on electronic direct marketing, that is via electronic message (e.g. email, SMS and MMS, *cf.* article 11.1(i) DTA). No prior consent is needed if the recipient is a legal entity or natural person acting in a professional capacity, provided that the contact details employed (i) had been made public for the purpose of receiving unsolicited direct marketing communications (for example, the use of an email address such as: [marketing@company.nl](mailto:marketing@company.nl)); or (ii) the permission for future use of those contact details had been obtained from the buyer in the context of a sale of a product or the performance of a service and the sender uses these contact details for the marketing of similar products or services, provided that the recipient was offered an opt-out when the contact details were initially collected (*cf.* article 13 e-Privacy Directive). In both instances, the contact details can only be used in accordance with the purposes for which they have been made public (article 11.7(2)(a) DTA).

#### **9.2 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 general prohibition of unsolicited communications imposed by article 11.7(1) DTA does not apply to unsolicited communications via telephone (article 11.7(5) DTA). Without prejudice to this exception, article 11.7(6) DTA provides for a national opt-out register containing the contact details of subscribers that have indicated that they do not wish to receive unsolicited communications as mentioned in article 11.7(5) DTA. Marketing companies are required to consult this register to be able to comply with the opt-out regime (see article 11.7(6–13) DTA).

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

The definition of the term ‘sender’ as used in article 11.7(1) DTA has

a broad meaning. For instance, if the transmission originates from outside of the Netherlands, but on instructions of a person (legal or natural) within the Netherlands, the instructor falls within the scope of the restrictions of article 11.7(1).

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

Both the Authority for Consumers and Markets (“ACM”) and the AP are increasingly active within the field of the enforcement of direct marketing restrictions. Indeed, the ACM nominated the protection of online consumers as one of the six priorities for the enforcement agenda of 2017.

#### **9.5 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 from third parties in itself is not prohibited. The subsequent use of the obtained contacts for the purpose of direct marketing is however restricted as the buyer will always require prior consent, which is a requirement under article 11.7(1) DTA.

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

The maximum penalty for sending marketing communications in breach of applicable restrictions differ depending on the applicable legal framework. With regard to breaches of the restrictions that arise from article 11.7 DTA, the maximum penalty is EUR 900,000.00 or 1% of the annual turnover (article 15.4(3) and article 15.1(3) DTA). However, fines for breaches of GDPR can go as high as EUR 20,000,000.00 or 4% of the annual turnover.

Both the ACM and the AP can also choose to impose an order subject to a penalty. Penalties related to such orders do not have a statutory limit.

## **10 Cookies**

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

The legal restrictions with regard to the use of cookies can be found in article 11.7a of the DTA, which implements Article 5 of the ePrivacy Directive. 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 Directive 95/46/EC and, from 25 May 2018, the GDPR). For consent to be valid, it must be informed, specific, freely given and must constitute a real 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, which means that it must be essential to fulfil their request.

Important to note is that insofar as personal data is processed by the use of cookies (for instance IP addresses), GDPR requirements may be applicable, such as the consent and transparency requirement.

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

The law makes exceptions on the beforementioned restrictions with regard to the use of certain types of cookies, specifically:

- a) cookies that are necessary for communication (e.g. load-balancing cookies) (article 11.7a(3)(a) DTA);
- b) cookies that are strictly necessary for the service requested by the user (article 11.7a(3)(b) DTA); and
- c) analytic, a/b testing and affiliate (performance) cookies, which are used for the purpose of obtaining information with regard to the effectiveness of a provided service, on the condition that the impact on the private life of the user is negligible (article 11.7a(3)(b) DTA).

With regard to these type of cookies, the information and consent requirements (article 11.7a(1)(a) and article 11.7a(1)(b) DTA) do not apply.

For the use of an additional type of cookie, namely Google Analytics cookies, the AP has outlined certain requirements surrounding consent and information obligations. This includes having a data processing agreement in place with Google, and that the user should be informed about the use of Google Analytics cookies.

The information and consent requirement in principle do apply to social media plug-in cookies.

Furthermore, the use of tracking cookies is presumed to be data processing unless the party that uses these cookies can prove otherwise (article 11.7a(4) DTA). The enforcement and supervisory tasks with regard to tracking cookies are primarily exercised by the AP, and not by the ACM.

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

The ACM and the AP have taken different enforcement actions with regard to the use of cookies. With regard to an online voting aid application ‘Stemwijzer’, the ACM and the AP combined their forces and addressed the use of certain advertisement cookies.

In 2017, the ACM addressed different medical websites to stop the use of cookies without the consent of the users of these websites. This was a year after the ACM urged the 100 most-used websites to change their cookie policies.

Furthermore, the AP ordered YD Display Advertising Benelux BV, under warning of a recurring penalty, to end its use of tracking cookies without the unambiguous consent of the data subjects involved.

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

The maximum penalty for breaches of the cookie restrictions differs depending on the applicable legal framework. Maximum penalties with regard to breaches of the restrictions that arise from article 11.7a DTA arise to EUR 900,000.00 or 1% of the annual turnover (article 15.4(3) and article 15.1(3) DTA). However, fines for breaches of the GDPR can go as high as EUR 20,000,000.00 or 4% of the annual turnover.

Both the ACM and the AP can also choose to impose an order subject to a penalty. Penalties related to such orders do not have a statutory limit.



## 11 Restrictions on International Data Transfers

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

Data transfers to a third country, i.e. countries that are not located within the European Economic Area (the “EEA”) can only take place if the European Commission has determined that this third country offers an adequate level of data protection, whether by its domestic legislation, or because of the international commitments that it has entered into as specified under the GDPR. Additionally, such transfers may take place if appropriate safeguards are established and on the condition that enforceable data subject rights and effective remedies for data subjects are available.

### 11.2 Please describe the mechanisms companies 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 third country, 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. These include:

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 that they have obtained prior approval by the relevant data protection authority.

International data transfers within a group of businesses can be safeguarded by the implementation of Binding Corporate Rules (“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 that 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.

Transfer of personal data to the US is also possible if the data importer has signed up to the EU-US Privacy Shield Framework, which was designed by the US Department of Commerce and the EU Commission to provide businesses in the EU and the US with a mechanism to comply with data protection requirements when transferring personal data from the EU to the US.

### 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 safeguards mentioned below will require prior approval from, in the Netherlands, the AP:

- Code of conduct.
- Certification mechanism.

- BCRs.
- Contractual clauses.
- Provisions inserted into administrative arrangements.

Article 49 of the GDPR provides for certain derogations for transfers (subject to requirements set out under article 49 of the GDPR). Transfers to other jurisdictions on the basis of an article 49 derogation requires prior notification to the relevant data protection authority, i.e. the AP in the Netherlands.

## 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 Article 29 Working Party (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. The WP29 recommends 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.

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

Anonymous reporting is not prohibited under EU data protection law; however, it raises problems concerning the essential requirement that personal data should only be collected fairly. As a rule, the WP29 considers 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.

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 DPIA must be undertaken (with the assistance from the DPO if appointed) 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 Dutch 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 put in place 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 will constitute a breach of the GDPR, it has to provide written advice to the controller within eight weeks of the request of a consultation. For this purpose, it can use any of its wider investigative, advisory and corrective powers as outlined in the GDPR.

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

The limitation on the purposes for which CCTV data may be used differs per the specific scenario in which CCTV is used, for instance, in public spaces in the municipality, in schools, in offices and in health care facilities. The AP has listed the limitations per scenario on its website. For government agencies, the purpose has to be directly linked to the statutory task of the respective body.

Moreover, in principle, it has to be established 1) who the controller is, 2) what the purposes are, 3) what the legal ground is, 4) that the use of CCTV is necessary, 5) which type of camera or software is justifiable, 6) what will be done with the footage, 7) the adequate security measures, 8) whether (and if so, how) the data subjects will be informed, and 9) that the data subjects should be able to exercise their rights. If these requirements are not sufficiently met, the use of CCTV is in principle not allowed.

## 14 Employee Monitoring

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

Employee monitoring is only permitted if there is a legitimate ground for it, which within the context of employee monitoring can be that it is necessary for purposes of the legitimate interests pursued by the data controller or a third party, except in the event that the interests or fundamental rights and freedoms of the involved employee prevails. Within this context, it should be noted that pursuant to case law of the European Court of Human Rights, the activities of an employee on the work floor are protected by privacy laws. Moreover, a complete prohibition of the use of an employer-provided email account for personal purposes is in general not acceptable under Dutch law.

Processing personal data based on the legitimate interest ground strictly requires a balancing of interests between the interest of the

data controller and the interests of the employee. In this respect, the sensitivity of the data processed and the measures taken by the data controller to limit the infringement of the employees' rights are important factors to consider. The nature, scope and form of the email investigation must be proportionate to the purposes of the internal investigation. The data controller will have to set out adequate safeguards to guarantee a careful use of the processed data.

The AP has issued some rules of thumb to assist employers with the weighing of interests in order to determine which circumstances will allow for the examining of emails. Relevant aspects to consider are:

1. *Transparency*: (i) has the employer informed the employees of the rules which apply to the use of email, including the use for private purposes; and (ii) has the employer been clear under which circumstances it may examine emails?
2. *Set clear purposes* for the intended investigation and *limit the investigation* strictly to these purposes:  
The investigation must be as limited as possible, for instance, (i) only review emails of employees who are suspected of committing irregularities, (ii) avoid opening private emails unless there is a reasonable indication that such private emails relate to the irregularities, and (iii) limit the scope of the investigation as far as possible (e.g. number of employees, number of emails and period in which the emails were sent).
3. Only conduct the email investigation if there are reasonably no other means which may have less impact on the privacy of the employees involved.

In sum: the investigation of emails must be tailor-made and must have a limited scope. This is in accordance with the Opinion (8/2001) of the WP29, stating that: "*All monitoring must be a proportionate response by an employer to the risks it faces taking into account the legitimate privacy and other interests of workers. Any personal data held or used in the course of monitoring must be adequate, relevant and excessive for the purpose of which the monitoring is justified. Any monitoring must be carried out in the least intrusive way possible.*"

It should be noted that under the Dutch Private Security Organisations and Detective Agencies Act (*Wet particuliere beveiligingsorganisaties en recherchebureaus*), it is in principle prohibited to carry out security/detective activities (including forensic IT services), except if carried out by a certified public accountant in the Netherlands. It should also be noted that the processing of sensitive personal data, such as data pertaining to an individual's race, health or criminal and unlawful behaviour, may not be processed at all. The UAVG does contain specific exemptions to this prohibition. However, these exemptions are not likely to apply in relation to the email investigation.

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

Transparency is a key principle of the GDPR. The general rule is that a data subject should be adequately informed about the fact that their data is being processed, by whom, and for what purposes.

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

Under Dutch law, companies with 50 (or more) employees are obliged to establish a works council. Pursuant to article 27, section 1 of the Dutch Works Council Act ("WCA"), the works council must be requested for its prior consent with respect to proposed decisions concerning the introduction, modification or withdrawal of regulations relating to, *inter alia*, (i) the processing and protection

of personal data of the persons who work for the company (article 27, paragraph 1, sub (k) WCA), and (ii) any arrangement for, or that may be used for, observation of or checking the presence, conduct or performance of persons who work for the company (article 27, paragraph 1, sub (l) WCA). The monitoring of employees' emails qualify as such regulations/arrangements and therefore requires the prior consent of the works council (provided that a works council is established).

## 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. According to article 5(f) of the GDPR, 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 (referred to as the 'integrity and confidentiality' principle).

Whilst neither Dutch law nor the GDPR provide specific requirements regarding the security measures to ensure the integrity and confidentiality of personal data, the AP did, in March 2013, publish more specific guidelines on the security measures that must be implemented pursuant to article 13 of the Wbp, referred to as the '*Richtsnoeren beveiliging persoonsgegevens*'. These guidelines, combined with the 'NEN-ISO/IEC 27002 2007-nl standards', provide fairly concrete guidance on how to determine which security measures must be implemented and concern both the controller as well as the processor.

Depending on the security risk, these 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) expects 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, i.e. the AP in the Netherlands, 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, i.e. generally within 24 hours.

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 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) expects 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 concerned.

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 (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). The UAVG excludes certain types of financial institutions from this obligation.

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

The maximum penalty is EUR 20 million or 4% of the company's worldwide turnover, whichever is the highest.

## 16 Enforcement and Sanctions

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

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
Investigative Powers	The AP has wide powers to order the controller and the processor to provide any information it requires for the performance of its tasks, which include to conduct investigations in the form of data protection audits, to carry out reviews on certificates issued pursuant to the GDPR, to access all personal data and information necessary for reviewing the performance of controllers' or processors' tasks, access to the premises of the data including any data processing equipment and to enter a dwelling without the occupant's consent.	

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
Corrective Powers	The AP has the authority 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, to order an incremental penalty and to impose coercive administrative action (as below).	
Authorisation and Advisory Powers	The AP 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.	
Imposition of Administrative Fines as well as Fines on the Basis of the Directors' Liability for Infringements of Specified GDPR Provisions	The GDPR provides for administrative fines which can be EUR 20 million or up to 4% of the business' worldwide annual turnover of the preceding financial year.	
Non-Compliance With a Data Protection Authority	The GDPR provides for administrative fines which will be EUR 20 million or up to 4% of the business' worldwide annual turnover of the preceding financial year, whichever is higher, as well as warnings, reprimands, order of penalty payments and administrative coercion.	

#### 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 58(2)(f) of the GDPR, the AP has the power to issue a temporary or permanent limitation or ban on certain processing activities. No prior court order is required for imposing such corrective sanctions (recital 129 GDPR). Moreover, said bans and limitations may usually take immediate effect, provided their proper notification in accordance with the relevant Dutch administrative provisions.

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

With regard to the AP's power to impose punitive fines, it is fair to say, judging from the AP's annual reports, that the AP rarely enforces this power (e.g. a total amount of zero in 2016 and 2017 combined). Furthermore, only a modest portion of the total amount of investigations initiated by the AP resulted in an order subject to a penalty for noncompliance or an administrative enforcement order

(e.g. ratio investigation: order 197:20 in 2016 and 200:20 in 2017). The AP has, however, reported a significant number of cautionary measures (i.e. sending warnings or conducting cautionary conversations with (alleged) infringers); to be precise, 303 in 2016, and 217 in 2017. A noteworthy case in this context concerns the AP's investigation into the alleged data processing infringement by the American company Airbnb. The online platform for leasing or renting short-term lodging ceased the unlawful processing of citizen service numbers at the insistence of the AP. The AP did not, however, issue a penalty order or a punitive fine, despite the fact that it had received about 100 complaints into the aforesaid processing activities of Airbnb. The foregoing conveys the impression that the AP leans towards alternative and non-punitive measures for the fulfilment of its enforcement task.

Some of the additional enforcement powers as described above have only been introduced under the GDPR (e.g. the power to impose a ban on particular processing activities). It is also worth noting that the budget of the AP is supposed to have doubled from its current number in the course of 2019, partly because of the expectation that the AP will require more capacity for its enforcement task under GDPR. At the same time, the Dutch parliament has urged the AP to, following the entry into force of the GDPR and UAVG, initially focus on providing guidance with regard to the implementation of these legislations, rather than to immediately and stringently take enforcement actions. In light of this request, as well as the expanded enforcement powers of the AP and its increased budget, it remains to be seen whether there will be a shift in the approach of the AP from the current norm.

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

Yes. An example in which the AP launched an investigation into an establishment outside of the Netherlands concerns the AP's investigation into WhatsApp. WhatsApp is based in California, the United States, and provides a service that is accessible to and expressly aimed at people in the Netherlands: the 'WhatsApp' app. The app is used by millions of Dutch smartphone users, and as it processes personal data, the AP is authorised to launch an investigation. To this end, the WP29 pointed out that the "[...] key point is that even if the local establishment is not involved in any direct way in the processing of data – as was the case here – the activities of that local subsidiary may still bring the data processing within the scope of EU data protection law, as long as there is an 'inextricable link' between the activities of the local establishment and the data processing. The CJEU's judgement suggests that revenue-raising in the EU by a local establishment, to the extent that such activities can be 'inextricably linked' to the processing of personal data taking place outside the EU, is sufficient for the Directive to apply to such processing by the non-EU controller."

The AP also actively participates in cross-border investigation. An example of a cross-border investigation concerns the current investigation into Uber. On 22 November 2017, the AP received a data breach notification from Uber. On 29 November 2017, the WP29 established a taskforce consisting of the national supervisory authorities of Belgium, Germany, France, Italy, Spain and the United Kingdom under the guidance of the AP. The AP is currently investigating the data breach across jurisdictions with the cooperation of the taskforce. A similar approach has been taken before with regard to investigations into Microsoft, Google, Facebook and Yahoo.

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

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

There is no formalised response to such requests. Typically, such requests are assessed in light of the legal grounds for the processing and transfer of personal data. Generally, an obligation arising from foreign law does not qualify as a legal obligation as referred to in article 6 of the GDPR. This legal obligation only relates to a legal obligation following from national or European legislation. In most cases, the legitimate interest seems to be the most suitable legal ground for the assessment of the most suitable response to such requests, as it allows the company approached to take adequate measures to ensure that only the necessary and relevant data is included in the transfer. Processing personal data based on this legal ground requires necessity. Further, it requires a balancing of interest test between the interests of the data controller or the third party (the company) involved and the interests of the data subject. The weighing of interests is the obligation of the data controller. This balancing of interest test should take into account issues of proportionality and subsidiarity.

Following from the WP29 Opinion 06/2014 on the notion of legitimate interest of the data controller under article 7 of Directive 95/46/EC, the key factors to be considered when applying the balancing test are: (a) the nature and source of the legitimate interest; (b) the impact on the data subjects; (c) provisional balance; and (d) additional safeguards applied by the controller to prevent any undue impact on the data subjects.

It is important to keep in mind that in the event that a foreign e-discovery request is granted and the receiving party is not located within the European Economic Area, appropriate safeguards must be ensured as prescribed by the GDPR.

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

The WP29 issued an opinion in 2009 (document 1/2009) on pre-trial discovery for cross-border civil litigation. Although the opinion was published nearly 10 years ago, it still provides insight into how a discovery request should be approached. This includes the guideline that a data transfer due to a discovery request must be based on legal grounds. It is doubtful whether consent can be given in such cases, but the WP29 recognises that there might be a legitimate interest for such a transfer. In such an event, a balancing of interest test should be conducted with the requesting party's interest on the one hand, and the data subject's interest on the other. The WP29 urges the parties involved to firstly issue such requests under the Hague Convention on the taking of evidence abroad in civil and commercial matters, as this is recognised as a formal basis for the transfer of personal data.

## 18 Trends and Developments

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

See section 16.

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

Judging from the annual report of the AP reflecting upon 2017, it is fair to say that the AP dedicated 2017 to preparing for the entry into force of the GDPR by 1) providing guidance with regard to the GDPR, and 2) reorganising in order to fulfil its broadened tasks under the GDPR. In total, the AP published 28 opinions, spoke to the press 658 times, and received a total of 9,501 questions and tips from the public in 2017. In order of popularity, these questions and tips primarily concerned the use of a citizen service number (*burgerservicenummer*, "BSN"), data transfers, data breaches, security and internet. Pending investigations, for instance regarding the data breach at Uber, concern similar 'hot topics'. The expectation is that these will remain important topics for the AP, alongside its focus on providing guidance to government bodies, organisations and data subjects with regard to their rights and obligations under the GDPR. This is also in line with what the parliament has urged the AP to do following the entry into force of the GDPR.

In accordance with the advice of the AP, the UAVG does not extensively elaborate on the norms of the GDPR. The AP feels that it is up to the European Data Protection Supervisor ("EDPS") to establish the definitive interpretation of the various directly applicable GDPR norms, which can then be assessed by the respective courts. Moreover, the Senate (*Eerste Kamer*) announced that it will adopt the UAVG on 15 May 2018 without, in principle, any further room for debate or votes (*Hamerstuk*). At the same time, however, the parliament has acknowledged that there are still open questions surrounding the UAVG (for instance, with regard to the age for consent). Another expectation is therefore that the AP will closely monitor relevant case law and challenges in order to provide guidance when the UAVG is revisited in early 2019.

The AP's international involvement is also an important focus for the AP, which included its participation in the WP29, giving input with regard to the upcoming ePrivacy Regulation and with regard to the Privacy Shield. The AP also initiated (together with the British supervisory authority the Information Commissioner's Office) the amendment of an existing enforcement cooperation agreement which includes the revision that national supervisory authorities will be allowed to determine themselves which data they wish to share internationally. The AP, together with the ICO and the Canadian supervisory authority, is expected to reveal its findings with regard to the feasibility of this international framework convention in October 2018 during the international convention for supervisory authorities.



**Kim Lucassen**

Loyens & Loeff N.V.  
Blaak 31  
3011 GA Rotterdam  
Netherlands

Tel: +31 10 224 64 16  
Email: [kim.lucassen@loyensloeff.com](mailto:kim.lucassen@loyensloeff.com)  
URL: [www.loyensloeff.com](http://www.loyensloeff.com)

Kim Lucassen, attorney-at-law and partner, is a member of the Litigation & Risk Management practice group. She specialises in data protection and privacy law, regulated markets and (international) contracts. Kim heads the Loyens & Loeff Data Protection & Privacy Team and the Life Sciences Team. She is also a member of the Privacy Law Association and of the International Association of Privacy Professionals (IAPP).

**Iram Velji**

Loyens & Loeff N.V.  
Blaak 31  
3011 GA Rotterdam  
Netherlands

Tel: +31 10 224 65 54  
Email: [iram.velji@loyensloeff.com](mailto:iram.velji@loyensloeff.com)  
URL: [www.loyensloeff.com](http://www.loyensloeff.com)

Iram Velji is a member of the Litigation & Risk Management practice group at Loyens & Loeff. She specialises in data protection and privacy law and life sciences. As a professional support lawyer, she functions as the central resource for research, know-how, case strategy, training as well as business development within the practice areas of Life Sciences and Data Protection & Privacy law. She is a member of the Privacy Law Association.



Loyens & Loeff N.V. is an independent full-service law firm specialised in providing legal and tax advice to enterprises, financial institutions and governments. Intensive cooperation between attorneys, tax advisers and civil law notaries places us in a unique position in our home markets, the Netherlands, Belgium, Luxembourg and Switzerland. We are the largest law firm in the Netherlands with our main offices in Amsterdam and Rotterdam, and have about 1400 employees worldwide. The principles of quality, transparency and short-line communication form the foundation for an informal and inspiring culture. This culture stimulates the search for pragmatic solutions to complex legal and tax issues.

The Loyens & Loeff firm-wide Data Protection & Privacy Team provides integrated Benelux and Swiss legal advice on a wide variety of complex privacy and data protection-related matters in all sectors, with a particular focus on the energy, financial institutions, automotive and healthcare sector, and such through a one-stop shop approach.



# Nigeria

Jackson, Etti & Edu

Ngozi Aderibigbe



## 1 Relevant Legislation and Competent Authorities

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

There are several legislations that contain data protection provisions; however, the most comprehensive statutory instrument on data protection is a subsidiary legislation made pursuant to the National Information and Technology Development Agency Act, 2007 (“NITDA Act”). The NITDA Act authorises the National Information and Technology Development Agency (“NITDA”) to develop guidelines for electronic governance and to monitor the use of electronic data interchange. Pursuant to this statutory mandate, NITDA has developed the 2013 Guidelines for Data Protection (“NITDA Guidelines”). The NITDA Guidelines stand out from other legislations because unlike other legislations that contain data protection provisions merely as ancillary to the legislations’ primary objectives, the NITDA Guidelines are principally for the purpose of prescribing guidelines for data protection.

There are views that suggest that the NITDA Guidelines are merely advisory and lack the force of law – these views may have been influenced by the permissive language of the Guidelines. However, it is important to note that, under Nigerian law, subsidiary legislations have the same force of law as their respective principal legislations and are therefore equally binding and enforceable. Therefore, in view of the fact that the NITDA Guidelines are a subsidiary legislation, having been enacted pursuant to the NITDA Act (the principal legislation), we believe that it is correct to find that the NITDA Guidelines have the force of law.

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

As with most jurisdictions, Nigeria’s data protection and privacy regime takes its earliest definition from the country’s constitution – the 1999 Constitution of the Federal Republic of Nigeria. Section 37 of the Constitution guarantees the protection of the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications. This protection is guaranteed as a fundamental right of every Nigerian citizen and is therefore the bedrock of Nigeria’s data protection regime.

Besides the NITDA Guidelines, the following legislations also preserve citizens’ right to privacy of personal data:

#### (a) The Freedom of Information Act 2011

The objective of this Act is to make public records and information held by Government agencies more freely accessible by the public. It does, however, create an exception with respect to personal records and information. Section 14 of the Freedom of Information Act restricts Government agencies from disclosing personal information by a public institution unless the individual’s consent is obtained, or the information is available to the public.

#### (b) The Child Rights Act 2003

The purpose of this Act is the protection of the Nigerian child, defined as persons under the age of 18 years. Section 3 of the Act reinforces the constitutional rights of every child as provided under the Constitution, which includes the right to privacy provided under section 37 of the Constitution. More specifically, section 8 of the Act guarantees the child’s right to privacy, subject to the parents’ or guardians’ right to exercise supervision and control the child’s conduct.

#### (c) Cybercrimes (Prohibition, Prevention, etc.) Act 2015

The Cybercrimes Act has as its general purpose the prevention and prosecution of cybercrimes. It places a duty on computer and mobile network and communication service providers to retain traffic data and subscriber information for a period of two years. It also requires such service providers to have regard to the individual’s right to privacy under the Constitution and to take measures to safeguard the confidentiality of data processing for the purpose of law enforcement.

The Cybercrimes Act also mandates financial institutions to put in place effective measures to safeguard the sensitive data of their customers.

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

The following sector-specific legislations contain certain data protection provisions:

#### The Telecommunication Sector: The Nigerian Communications Commission Consumer Code of Practice Regulations 2007

The Nigerian Communication Commission (“NCC”) is the regulatory body for the telecommunications industry in Nigeria. Pursuant to powers conferred by its enabling Act – the Nigerian Communications Commission Act 2003 (“NCC Act”) – the NCC has published the NCC Consumer Code of Practice Regulations 2007 for telecommunication service providers. The Schedule to the NCC Consumer Code of Practice contains the General Consumer Code of Practice. This Code applies only to providers of

communication services in Nigeria. It sets out principles to regulate the collection and maintenance of consumers' personal information and requires such service providers to ensure the protection of such information. The Code further requires telecommunication companies to implement appropriate policy to ensure proper collection, use and protection of consumer information, and to ensure that third parties with whom telecommunication companies transact with have adopted appropriate measures for the protection of consumer information.

The NCC Consumer Code of Practice Regulations 2007 is being revised.

The Telecommunication Sector: Nigerian Communications Commission (Registration of Telephone Subscribers) Regulations 2011

The Nigerian Communications Commission (Registration of Telephone Subscribers) Regulations 2011 ("Registration of Telephone Subscribers Regulation") are applicable to telecommunications companies. Regulations 9 and 10 of the Registration of Telephone Subscribers Regulation contain data protection provisions. Regulation 9 guarantees the confidentiality of subscriber information held in the NCC's Central Database. It also recognises the subscriber's right to view and update their personal information held in the NCC's Central Database or the database of any telecommunication company.

The Financial Sector: Central Bank of Nigeria's Consumer Protection Framework 2016

The Central Bank of Nigeria's Consumer Protection Framework 2016 ("CBN Consumer Protection Framework") is a subsidiary legislation made pursuant to the Central Bank of Nigeria Act of 2007. Section 6(2) of this subsidiary legislation imposes a burden on financial institutions to maintain the confidentiality and privacy of all financial services customers – present or past. Appropriate data protection measures and staff training programmes are to be put in place to prevent unauthorised access, alteration, disclosure, accidental loss or destruction of customer data. Financial services providers are also required to obtain the written consent of consumers before their data is shared with third parties or used for promotional offers.

The Financial Sector: Credit Reporting Act of 2017

The Credit Reporting Act of 2017 provides a framework for credit reporting by credit bureaux. Section 5 of the Act requires credit bureaux to maintain credit information for at least six years from the date on which such information was obtained, after which the information should be archived for a further period of 10 years. It may thereafter be destroyed by the credit bureau. Section 9 of the Act reiterates the rights of data subjects (i.e. persons whose credit data are held by a credit bureau) to the privacy, confidentiality and protection of their credit information, and prescribes the preconditions under which data subjects' credit information may be disclosed.

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

There is no designated general regulator for data protection in Nigeria. Thus, the regulators for specific legislations are deemed to have authority to enforce data protection provisions of the respective legislations.

Regulator	Legislation
Nigerian Information Technology Development Agency (NITDA)	■ The NITDA Guidelines for Data Protection 2013

Regulator	Legislation
Nigerian Communications Commission (NCC)	■ Nigerian Communications Commission (Registration of Telephone Subscribers) Regulations 2011 ■ The NCC Consumer Code of Practice Regulations 2007
Central Bank of Nigeria (CBN)	■ Central Bank of Nigeria's Consumer Protection Framework 2016 ■ Credit Reporting Act of 2017

## 2 Definitions

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

#### ■ "Personal Data"

The NITDA Guidelines define personal data to mean any information relating to an identified or identifiable natural person ("data subject"). It includes information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, address, a photo, an e-mail address, bank details, posts on social networking websites, medical information, and other unique identifiers such as, but not limited to, a MAC address, IP address, IMEI number, IMSI number, SIM and others.

The data protection provisions contained in the Registration of Telephone Subscribers Regulation use the phrase "personal information" which is defined therein as the full names (including mother's maiden name), gender, date of birth, residential address, nationality, state of origin, occupation and such other personal information and contact details of subscribers.

#### ■ "Processing"

"Processing of Personal Data" is defined under the NITDA Guidelines to mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

#### ■ "Controller"

The NITDA Guidelines define "data controller" to mean any person, public authority, agency or any other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by an Act of National Assembly or regulations, the controller or the specific criteria for his nomination will be as stated by the Act or regulation.

#### ■ "Processor"

This term is not defined in the NITDA Guidelines nor in any other relevant legislation.

#### ■ "Data Subject"

Under the NITDA Guidelines, "data subject" means an identifiable person; one who can be identified directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

#### ■ "Sensitive Personal Data"

This means data relating to religious or other beliefs, sexual orientation, health, race, ethnicity, political views and trade-union membership.

#### ■ “Data Breach”

This term is not captured in the NITDA Guidelines or any other relevant legislation.

#### ■ *Other key definitions – please specify (e.g., “Pseudonymous Data”, “Direct Personal Data”, “Indirect Personal Data”)*

The following definitions are provided in the NITDA Guidelines:

- “**Data Subject’s Consent**”: this means any freely given specific and informed indication of a data subject’s wishes by which the data subject signifies his agreement to personal data relating to him being processed.
- “**Personal Data Filing System**”: means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed.
- “**Data Portability**”: means the ability for data to be transferred easily from one IT system to another through a safe and secure means in a standard format.

### 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 NITDA Guidelines extend to organisations outside Nigeria to the extent that such organisations process personal data of Nigerian citizens.

### 4 Key Principles

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

##### ■ Transparency

Where personal data has been obtained otherwise than from the data subject, sections 2.1(3) and 2.2(3) of the NITDA Guidelines place a requirement on the data controller to disclose to the data subject the following information, except where the data subject already has it:

- the identity of the controller and of the representative, if any;
- the purpose for which the data is being processed; and
- any further information, such as the categories of data concerned, the recipients or categories of recipients, the existence of the mechanism for access to, and mechanism for rectifying, the data subject’s data.

In addition, section 2.1(9) of the Guidelines provides that a data subject should be able to obtain from data controllers, without constraint, information on the data subject’s personal data being processed, including the category of data, identity of any third-party recipients of the data, the source of the data, the procedure for any automatic processing of data, etc.

Section 4.1.1 of the NITDA Guidelines also requires data controllers to inform data subjects about the purpose for which the data is being collected. If the data is to be sent outside Nigeria, the data controller is expected to inform the data subjects of this fact.

The NCC Consumer Code of Practice Regulation 2007 provides that any telecommunication service operator that collects information on individual consumers should have an accessible and easy-to-read policy on the protection of consumer information. The policy should state clearly what information is being collected; the use of that information;

possible third-party exchange or disclosure of that information; and the choices available to the consumer regarding collection, use and disclosure of the collected information.

##### ■ Lawful basis for processing

Section 2.1(8) of the NITDA Guidelines provides that personal data may be processed only under one of the following conditions:

- if the data subject has unambiguously given his or her consent to the processing;
- the processing is necessary in furtherance of a contract to which the data subject is a party;
- the processing is necessary for compliance with a legal obligation to which the controller is subject to;
- the processing is necessary to protect the vital interests of the data subject;
- the processing is necessary in the public interest or in the exercise of the controller’s official authority;
- the processing is required for health management purposes and the data is processed by a health professional who is subject to the obligation of professional secrecy;
- the processing is in connection with any offences, criminal convictions, etc;
- the data is processed in connection with administrative sanctions or judgments in civil cases; or
- the processing is necessary for the purpose of the legitimate interests pursued by the data controller or by the third party or such parties to whom the data is disclosed.

The NITDA Guidelines provide eight principles for data protection, the first of which is that personal data must be processed fairly and lawfully. The Guidelines require data controllers to inform data subjects about the purposes for which data is being collected. If the data is to be transferred outside of Nigeria, this fact should also be made known to the data subjects.

The NCC General Consumer Code of Practice Regulations 2007 mandate telecommunication services operators to collect and maintain information on individual consumers in a fair and lawful manner. To this end, telecommunication services operators are required to provide: notice to consumers on the information they collect, and its use or disclosure; the choices consumers have with regard to their personal data; access by consumers to their data; and security measures taken to safeguard consumer’s information.

##### ■ Purpose limitation

The NITDA Guidelines restrict the use of personal data to the purpose for which the data was collected. Principle 2 stated in section 4.1.2 of the Guidelines requires data controllers to ensure that data collected for one purpose is not used for a different purpose. The purpose for collecting the data must be reasonable and obviously lawful.

Telecommunication companies are required by the NCC Consumer Code of Practice Regulations to process individual consumers’ information for limited and identified purposes. Similarly, Regulation 9 of the NCC (Registration of Telephone Subscribers) Regulations restrains telecommunication companies from using personal information of subscribers in any manner other than for the company’s operations and in line with the NCC Consumer Code of Practice.

##### ■ Data minimisation

The NITDA Guidelines prevent data controllers from collecting excessive data. Only such data as is necessary, bearing in mind the purpose of the data collection, should be collected by data controllers.

##### ■ Proportionality

This term is not captured in the NITDA Guidelines or any other relevant legislation.

## ■ Retention

There is no generally applicable timeline for data retention. The NITDA Guidelines provide that personal data should be kept for no longer than is necessary. It requires data controllers to develop a retention policy for data. A similar provision is contained in the NCC's General Code, which prevents telecommunications companies from keeping information for longer than is necessary.

The Credit Reporting Act specifically requires credit bureaux to maintain credit information for at least six years from the date on which such information was obtained, after which the information should be archived for a further period of 10 years. It may thereafter be destroyed by the credit bureau.

Section 38 of the Cybercrimes Act mandates companies that provide communication services or that process or hold computerised data to keep all traffic data and subscriber information for a period of two years.

## ■ Other key principles – please specify

Besides the principles already discussed above, the following Principles are provided for in the NITDA Guidelines:

- (i) Principle 4 – Personal data must be accurate and where necessary kept up to date: This principle requires data controllers to provide data subjects with the option of and a means to update their personal data.
- (ii) Principle 6 – Personal data must be processed in accordance with the rights of the data subject: Data subjects are entitled to request to view their data as held by the data controller, and the data controller is required to respond to such requests without delay.
- (iii) Principle 7 – Appropriate technical and organisational measures must be established to protect the data.
- (iv) Principle 8 – Personal data must not be transferred outside Nigeria unless adequate provisions are in place for its protection in the receiving country.

## 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 the NITDA Guidelines, individuals have the right to request for copies of their data which should be made available within seven days of request.

Section 9(6)(a) of the Credit Reporting Act gives data subjects the right to request for their credit information, which is classified as personal data. Also, under the Registration of Telephone Subscribers Regulation, any telecommunication services subscriber whose personal information is stored by the service provider is entitled to view the said information and to request updates and amendments to the information.

#### ■ Right to rectification of errors

Under the NITDA Guidelines, individuals have the right to obtain from the data controller rectification of data not in compliance with the Guidelines. Also, they are entitled to the notifications sent to third parties to whom the data in need of rectification have been disclosed. Principle 4 under the NITDA Guidelines requires that personal data be accurate and kept up to date. Thus, data controllers are expected to provide individuals with the ability to update or correct their personal data as the need arises.

The Credit Reporting Act, in section 9(6)(b), gives data subjects the right to contest the accuracy of their credit information within 15 days of receiving the credit report, and to have the matter resolved promptly. Also, under the

Registration of Telephone Subscribers Regulation, any telecommunication services subscriber whose personal information is stored by the service provider is entitled to request updates and amendments to the information.

#### ■ Right to deletion/right to be forgotten

There are no clear provisions on a data subject's right to deletion or right to be forgotten under any of the relevant legislations. However, the NITDA Guidelines provide that data subjects should be able to rectify, erase or block data which does not comply with the provisions of the Guidelines.

#### ■ Right to object to processing

The NITDA Guidelines provide that data subjects should have the option to object to and request free of charge the processing of personal data relating to him which the data controller intends to process for the purpose of direct marketing. Individuals have the right to object to processing of data for the purpose of direct marketing and also to object to disclosure of data to a third party.

The CBN Consumer Protection Framework states that the consent of consumers shall be obtained in writing before their data is shared with third parties, and before using such information for future promotional offers via e-mail, SMS, phone calls and other channels.

#### ■ Right to restrict processing

Under the NITDA Guidelines, data subjects should have the option to object to the processing of his or her personal data for the purposes of direct marketing.

#### ■ Right to data portability

Under the NITDA Guidelines, a data subject is entitled to obtain from the data controller a copy of his or her personal data in a format usable by the data subject. The data subject is also entitled to request that his or her data be transmitted electronically to another processing system.

#### ■ Right to withdraw consent

Under the NITDA Guidelines, individuals are entitled to opt out if data processing is for the purpose of marketing communications.

#### ■ Right to object to marketing

The NITDA Guidelines provide that individuals should have the right to object to the processing of data for the purpose of direct marketing or opt out of marketing communications.

#### ■ Right to complain to the relevant data protection authority(ies)

The NITDA Guidelines are silent on the individual's right to complain.

However, the Credit Reporting Act of 2017 provides in Part IV, section 13 that a data subject having complaints regarding the accuracy of the credit information shall submit the complaint in writing to the credit information provider.

#### ■ Other key rights – please specify

There are no other specific key rights.

## 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 NITDA Guidelines do not impose an obligation on a business to register or notify NITDA regarding its data processing activities. Some sector-specific authorities require registration, but this is



mainly to enable the exercise of the Regulator's supervisory role over the regulated entities and not in relation to data processing.

**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?**

This is not applicable in our jurisdiction.

**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 NITDA Guidelines require organisations to appoint Data Security Officers.

**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 Security Officer; however, the general sanction prescribed under the NITDA Act which is applicable to breach of any guidelines made by NITDA (of up to ₦200,000) may be imposed.

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

There is no provision for the immunity of the officer from disciplinary measures in the NITDA Guidelines.

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

The NITDA Guidelines have no express provision as to extent of the Data Security Officer's mandate. However, it does state that organisations shall designate an employee of that organisation as the organisation's Data Security Officer.

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

Being an employee of the subject organisation is the only qualification for a Data Security Officer under the NITDA Guidelines.

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

The Data Security Officer's duties shall include the following:

- Ensuring that the organisation adheres to the NITDA Guidelines.
- Ensuring continued adherence to data protection and privacy policies and procedures.
- Ensuring that personal data is protected and providing for effective oversight of the collection and use of personal information.
- To be responsible for effective data protection and management within the organisation and ensure compliance with the privacy and data security policies.
- Providing training and education for employees to promote awareness of and compliance with the privacy and data security policies.



- f. Developing recommended practices and procedures to ensure compliance with the privacy and data security policies.

#### 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 registration of Data Security Officers in the applicable legislations.

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

There is no obligation to name the Data Security Officer in the organisation's 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?

The NITDA Guidelines require that a data controller who engages the services of another entity to process personal data must have a contract in place with the third-party 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 agreement is required to be in writing and should stipulate that the third-party processor would act only on instructions from the data controller. It should also restrict the data processor from transferring personal data outside Nigeria unless the receiving country ensures an adequate level of protection.

### 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 NITDA Guidelines require data controllers to pre-notify data subjects before their personal data is used for marketing communications. Data subjects should also have an opt-out option from such communications.

#### 9.2 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 addition to the aforementioned restriction under the NITDA Guidelines, the NCC Consumer Code of Protection restricts telecommunication companies from telemarketing unless they make the following disclosures: the third party on whose behalf it is made and the purpose of the communication; the full price of the product

or service which is being marketed; and confirmation that the individual has an absolute right to cancel the agreement for purchase, lease or other supply of any product or service within seven days of the communication, by calling a stated toll-free telephone number. The NCC has also recently mandated all telecommunication service providers to activate a DO-NOT-DISTURB shortcode which allows consumers to opt out of telemarketing communications.

#### 9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

There is no specific provision for marketing from other jurisdictions. However, it would appear that marketing from foreign jurisdictions which are delivered to consumers through local telecommunication service providers would be caught by the above provisions of the NCC Consumer Code.

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

The NCC is relatively active in the enforcement of breaches of Consumer Codes. NITDA is however not active in enforcing the NITDA Guidelines.

#### 9.5 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 specific provision on purchasing marketing lists. However, the provisions relating to the data subject consents as provided under the NITDA Guidelines and other relevant legislations must be complied with. For example, the NCC Consumer Code of Practice Regulations and the Registration of Telephone Subscribers Regulation prevent telecommunication service providers from granting third-party access to consumers' personal information, except as agreed with the consumer or subject or as provided in the Regulations.

#### 9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

There are no specific penalty provisions in the NITDA Guidelines for marketing communications in breach of the Guidelines. However, by section 17(4) of the NITDA Act, where an organisation fails to comply with the guidelines and standards prescribed by NITDA (including the NITDA Guidelines), such organisation commits an offence and may be liable on conviction to a fine of ₦200,000 or imprisonment for a term of one year or both for first time offences; for a second and subsequent offence, to a fine of ₦500,000 or imprisonment for a term of three years or both.

With respect to telecommunication operators, the Nigerian Communications (Enforcement Processes, etc.) Regulations of 2005 have a general provision which penalises telecommunication operators for any breach of any regulations put forth by the NCC. A fine of ₦10,000,000 is the sanction for such breach.

### 10 Cookies

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

There is no direct legislative restriction on the use of cookies. However, it is relevant to mention that the Cybercrime Act makes it a crime

for a person with intent to defraud to use any device or attachment (including cookies) to obtain information or details of a cardholder.

**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 our jurisdiction.

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

This is not applicable in our jurisdiction.

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

This is not applicable in our jurisdiction.

## 11 Restrictions on International Data Transfers

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

The NITDA Guidelines restrict the transfer of personal data outside Nigeria unless adequate provisions are in place for its protection in the receiving country.

**11.2 Please describe the mechanisms companies 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, the level of compliance with the provisions of the NITDA Guidelines leaves much to be desired. However, the Guidelines provide that data controllers should consider the following questions in deciding whether personal data should be transferred outside Nigeria:

- (a) Does the receiving country have adequate Data Protection Guidelines legislation equivalent to that of Nigeria?
- (b) Is it necessary to send the data as part of the fulfilment of a contract?
- (c) Has the data subject consented? (Does the fair processing notice include a statement to the effect that it may be transferred outside Nigeria?)
- (d) Is the data being processed by another office of the same firm which is established within Nigeria?
- (e) Is there a contract in place between the data controller and the receiving organisation providing for adequate protection of personal data?

**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 NITDA Guidelines do not provide for notification or prior approval for transfer of data outside Nigeria.

## 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 applicable legislations have no provision on whistle-blowing.

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

This is not applicable in our jurisdiction.

## 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)?**

As part of the application of Principle 1 (personal data must be processed fairly and lawfully), the NITDA Guidelines provide that notices on the purpose and scope of data collection should be displayed prominently where CCTV is used.

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

The applicable legislations have no provision limiting the purpose 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?**

There are no specific provisions for employee monitoring. Thus, employee monitoring would be subject to the general provisions on data protection and the individual's rights to privacy.

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

This is not applicable in our jurisdiction.

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

This is not applicable in our jurisdiction.

### 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 responsibility to keep personal data secure is placed on the data controller by virtue of the NITDA Guidelines. Under the Registration of Telephone Subscribers Regulation and the Consumer Code of Practice Regulations, the duty to ensure security of personal data is on the telecommunication operator.

#### 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) expects voluntary breach reporting.

The NITDA Guidelines make no provision in this regard.

#### 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) expects voluntary breach reporting.

There are no specific provisions requiring notice of the data breaches to be sent to data subjects.

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

There is no specific penalty provision in the NITDA Guidelines for breach of data security. However, if such breaches result from noncompliance with any provision of the NITDA Guidelines, then the penalty provisions in the NITDA Act becomes relevant. The NITDA Act provides for liability of up to ₦200,000 or imprisonment for a term of three years or both; such fine and imprisonment for breach of guidelines and standards issued by NITDA.

### 16 Enforcement and Sanctions

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

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
<p><u>Cybercrimes Act 2015:</u></p> <p>The Office of the National Security Adviser is to coordinate the administration of the provisions of the Act, while the Attorney General is to ensure effective prosecution of cybercrimes.</p>	No administrative sanctions.	<p>The Act in section 21 provides the sanction for any person who fails to have due regard for an individual's right to privacy and safeguard the confidentiality of the data processed. On conviction, the person shall be liable to imprisonment for a term of not more than three years or a fine of not more than ₦7,000,000, or both.</p>
<p><u>The NCC Consumer Code of Practice Regulation 2007:</u></p> <p>Responsible for the enforcement of data protection provisions under this Regulation is the NCC. The NCC's investigatory power includes the conduct of quarterly audits, inspections and monitoring of licensed telecom operators to ensure compliance with its codes and regulations.</p>	This is inclusive of issuance of caution notices to a licensee with no past record, but in the case of continuing breach, the Commission shall determine if they constitute an offence under the NCC Act, including as a breach of applicable licence conditions.	<p>Section 55(3) refers to the Nigerian Communication (Enforcement Processes, etc.) Regulations with respect to penalties for contravening the Code. A fine of ₦10,000,000 is the sanction for such breach.</p>
<p><u>National Information and Technology Development Agency Act, 2007:</u></p> <p>The NITDA Act saddles NITDA with the responsibility of investigating and enforcing the provisions of the NITDA Guidelines.</p>	The NITDA Guidelines have no specific applicable administrative or civil sanctions.	<p>A breach of the NITDA Guidelines is a breach of the provisions of the NITDA Act which is an offence under section 17(4) of the NITDA Act. Upon conviction, the individual or body corporate in breach is liable to pay a fine of ₦200,000 or imprisonment for a term of one year, or both, if a first offence. If a subsequent offence, a fine of ₦500,000 or imprisonment of three years, or both.</p>
<p>The Credit Reporting Act of 2017 vests on the Central Bank of Nigeria investigatory power for breaches of the provisions of the Act.</p>	Section 14(e) of the Credit Reporting Act of 2017 states that the Central Bank may revoke a credit bureau's licence if it breaches the provisions of law on data protection.	<p>Section 20(1)(c) of the Act states that a person who intentionally or negligently discloses credit information commits an offence. It is punishable under section 23 with a fine of not less than ₦10,000,000 or imprisonment for a term of 10 years, or both.</p>

---

**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 respective regulatory authorities that exercise oversight over legislations with data protection provisions would have power to ban a data processing activity provided that such a ban falls within the statutory powers of the regulatory authority. A court order is not required.

---

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

---

The usual approach would be by issuing policies applicable to organisations within the regulator's supervisory control.

---

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

---

The respective regulatory authorities may exercise its powers against foreign companies to the extent that the activities of such companies affect the regulated sector. In some cases, regulators may penalise foreign companies by preventing or limiting their continued operation within Nigeria.

---

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

---



---

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

---

There is no specific rule on how Nigerian companies may respond to foreign e-discovery or disclosure requests.

---

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

---

There has been no guidance.

---

## **18 Trends and Developments**

---



---

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

---

The “enforceability” of the NITDA Guidelines has remained a subject of debate in many circles, largely because of the permissive language predominantly used in the Guidelines. The debate is exacerbated by NITDA's apparent docility in enforcing the provisions of the NITDA Guidelines. There is an increasing call for a full-fledged, principal legislation on data protection to be enacted by the National Assembly and the creation of a Government agency with specific responsibility for data protection. It is believed that having such a primary federal legislation on data protection and a corresponding regulatory agency would significantly strengthen Nigeria's data protection regime.

---

**18.2 What “hot topics” are currently a focus for the data protection regulator?**

---

The NITDA Guidelines are currently being updated and reviewed and it is hoped that the updated Guidelines would provide more clarity on the legal status of the Guidelines. NITDA recently confirmed that the reviewed Data Protection Guidelines are currently at the stage of stakeholder consultation.



**Ngozi Aderibigbe**

Jackson, Etti & Edu  
RCO Court  
3–5 Sinari Daranijo Street  
Victoria Island  
Lagos  
Nigeria

Tel: +234 4626 841-3  
Email: [ngoziaderibigbe@jacksonettiedu.com](mailto:ngoziaderibigbe@jacksonettiedu.com)  
URL: [www.jacksonettiedu.com](http://www.jacksonettiedu.com)

Ngozi is an intellectual property and commercial law expert. She heads the Technology, Media & Entertainment sector practice at Jackson, Etti & Edu, Nigeria's leading full-service law firm.

Ngozi is involved in providing advice on data protection to local and foreign technology companies. She provides thought leadership on privacy and data protection and its application in today's data-driven business environment.

As a technology savvy lawyer, Ngozi keeps abreast of developments in the technology sector and is knowledgeable about emerging technologies and the applicable legal framework for such technologies. She supports technology companies at every stage of their business cycle – whether as startups or established technology companies. Ngozi also advises on the regulatory framework for companies that create technology, are enabled by technology or whose business model are built around technology.



Jackson, Etti & Edu is a full-service law firm with a sector focus, rendering legal services to Nigerian, Pan-African and International clients in diverse jurisdictions. With over 20 years of valuable experience, our lawyers have gained extensive experience in advising and acting for clients on a wide range of subject matters.

Our firm is recognised for professional legal services of the highest calibre. We draw on our unique knowledge of the African business environment, and in-depth understanding of the economic and socio-political climate in advising clients on a wide range of legal issues.

**Sector Focus**

One of our key differentiating factors is our strong sector-focused approach. Our key sectors are:

- Energy & Natural Resources.
- Fast Moving Consumer Goods (FMCGs).
- Financial Services.
- Health & Pharmaceuticals.
- Real Estate & Infrastructure.
- Technology, Media & Entertainment.

**Our practice areas are:**

- Banking & Finance.
- Commercial Intellectual Property.
- Corporate Commercial & General Legal Advisory.
- Litigation & Dispute Resolution.
- Immigration Advisory & Compliance.
- Intellectual Property.
- Real Estate.
- Regulatory & Compliance.

# Norway

Wikborg Rein Advokatfirma AS

Line Coll



Vilde Juliussen



## 1 Relevant Legislation and Competent Authorities

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

From 25 May 2018, the principal data protection legislation in the EU will be Regulation (EU) 2017/679 (the “General Data Protection Regulation” or “GDPR”). The GDPR repeals Directive 95/46/EC (the “Data Protection Directive”) and leads to increased (though not total) harmonisation of data protection law across the EU Member States. As Norway is not an EU Member State, the GDPR must first be incorporated into the European Economic Area (“EEA”) Agreement before it can be implemented as national law in Norway by means of a new Personal Data Act. The Norwegian government is making its best efforts to ensure that the regulation shall start to apply in Norwegian law simultaneously with the EU Member States or shortly thereafter. A bill proposing a new Personal Data Act, and implementing the GDPR by referring to its incorporation in the EEA Agreement, was presented in Parliament on 23 March 2018. Due to a delay in the process of incorporating the GDPR into the EEA Agreement, the expected effective date for the regulation in Norway is now 1 July 2018.

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

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 Directive 2002/58/EC (as amended by Directive 2009/136/EC) (the “ePrivacy Directive”).

In addition, the Marketing Control Act regulates marketing communications (see question 9.1).

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

Various sectorial legislations will 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 Records (Act of 20 June 2014 No. 42), the Health Research Act (Act of 20 June 2008 No. 44), the 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), the Schengen Information Systems Act (Act of 16

July 1999 No. 66) and its regulations, and the Currency Exchange Register Act (Act of 28 May 2004 No. 29) will also impact data protection. The Ministry of Justice and Public Security (hereinafter referred to as the “Ministry”) proposes to maintain these sector-specific laws also after the implementation of the GDPR, but to amend the relevant provisions in order to secure 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 will continue to hold this responsibility when the GDPR is implemented. 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.

In the case of medical and health research on human beings or human biological material, an application for approval of the research project should be made to the Regional Committee for Medical and Health Research Ethics (“REK”) in the applicant’s geographical area, according to the Health Research Act. Today, prior approval from REK is regarded as a necessary and adequate legal ground for the processing of health data in medical and health research. After the implementation of the GDPR, however, such prior approval will no longer be regarded as a necessary and adequate legal ground for the processing of health data and such processing must be based on one of the grounds in Article 9(2).

Data controllers within the health sector are also regulated by the various health sector legislations relating to the processing of medical health data (see question 1.3).

The Norwegian Communications Authority 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”

“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.

#### ■ 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 “data that directly identify a natural person” (*direkte personidentifiserbare opplysninger*). 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 proposed 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 proposed Personal Data Act.

The proposed 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 interest 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.

## ■ Other key principles – please specify

### 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.

#### ■ 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

#### 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.

#### Automated individual decision-making

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?

The general rule prior to the implementation of the GDPR into Norwegian law is that all processing of identifiable personal data is subject to a duty to notify such processing to the NDPA unless the processing is: (a) subject to an obligation to obtain a licence from the NDPA; or (b) exempted from the obligation to obtain a licence or to notify pursuant to the Personal Data Act of 2000. As the GDPR removes the obligation to notify the data protection authority in respect of processing activities, the Ministry has proposed not to pursue this obligation in the new Personal Data Act incorporating the GDPR. Consequently, there will be no general legal obligation on businesses to register with or notify the NDPA in respect of its processing activities after the implementation of the GDPR.

Please note, however, that in the case of medical and health research on human beings or human biological material, an application for approval of the research project should be made to the Regional Committee for Medical and Health Research Ethics ("REK") in the applicant's geographical area, according to the Health Research Act; see question 1.4 above.

### 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 after the implementation of the GDPR into Norwegian law.

### 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 after the implementation of the GDPR into Norwegian law.

### 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 after the implementation of the GDPR into Norwegian law.

### 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 after the implementation of the GDPR into Norwegian law.

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

This is not applicable after the implementation of the GDPR into Norwegian law.

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

This is not applicable after the implementation of the GDPR into Norwegian law.

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

This is not applicable after the implementation of the GDPR into Norwegian law.

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

No prior approval from the data protection regulator will be required after the implementation of the GDPR, but the Ministry proposes a provision entitling the King in Council (the government) to adopt regulations that allow the processing of sensitive 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. Such processing will require authorisation by the NDPA.

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

This is not applicable after the implementation of the GDPR into Norwegian law.

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

This is not applicable after the implementation of the GDPR into Norwegian law.

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

This is not applicable after the implementation of the GDPR into Norwegian law.



## 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.

Once the GDPR is incorporated into Norwegian law, 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 sensitive 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 Data Protection Bill, the Justice Department states that this comprises the administrative bodies that fall within the second sentence of section 1 of the Public Administration Act, i.e., any state 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 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 to 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 ("DPIA") and the training of staff; and (iv) co-operating 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 stated that, after the implementation of the GDPR into Norwegian law, it will set up a registration system where organisations can register the contact details of the 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. Furthermore, the GDPR requires that the contact details of the Data Protection Officer shall be published. As a matter of good practice, the WP29 recommends that an organisation informs its employees of the name and contact details of the Data Protection Officer. The WP29 also holds 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 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?)

According to the Marketing Control Act, consumers may opt out of marketing by telephone or addressed mail by registering their names, addresses and telephone numbers in the Central Marketing Exclusion Register. Both consumers and other natural persons may opt out by contacting the trader directly. Telephone marketing on Saturdays, Sundays, public holidays or on weekdays before 09:00 or after 21:00 is prohibited.

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 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.)

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 mail.

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 costs can opt out of marketing directly with the trader.

### 9.3 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.

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

No, compliance with the provisions mentioned in questions 9.1 to 9.3 above of the Marketing Control Act is monitored by the Consumer Authority (formerly known as the Consumer Ombudsman) and the Market Council.

### 9.5 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 mail provided that the conditions, restrictions and prohibitions specified in question 9.2 are adhered to.

In practice, marketing lists from third parties can 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 to what extent. 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.

### 9.6 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 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) 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. As long as there is clear information available on the website itself about what cookies are used, which information is processed, the purpose of the processing and who is processing the data, consent may be given by the end user making use of a technical setting in the web browser or similar measure. A pre-setting in the web browser that the user accepts cookies is deemed to be consent. It is sufficient that the user consents once for the same purpose. The user must have the possibility to withdraw his/her consent.

### 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, the Norwegian Communications Authority initiated a review of Norwegian websites to determine how such websites are implementing the requirements of the aforementioned section 2-7 b. The Norwegian Communications Authority looked at the 500 most-visited Norwegian websites. Four out of five of the investigated websites were found to be non-compliant. The Authority contacted the non-compliant websites and stated that it will 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 are the issue of an order to rectify one’s position and/or 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, 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 1,130), i.e., up to NOK 33,900.

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), once this is implemented in Norwegian law, 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 companies 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.).

After the incorporation of the GDPR into Norwegian law, 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 complaint procedures.

Transfer of personal data to the US is also possible if the data importer has signed up to the EU-US Privacy Shield Framework, which was designed by the US Department of Commerce and the EU Commission to provide businesses in the EU and the US with a mechanism to comply with data protection requirements when transferring personal data from the EU to the US.

**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 international data transfer will require prior approval from the relevant data protection authority unless the controller or processor has 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 relevant data protection authority, such as the establishment of BCRs.

## 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. Workers hired from temporary-work agencies also have a right to notify censurable conditions at the hirer's undertaking. According to section 2 A-3, if the conditions at the undertaking so indicate, the employer shall be obliged to prepare procedures for internal notification in connection with systematic health, environment and safety work. Such procedures must always be prepared if the undertaking regularly employs five or more employees. Such 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, or strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do companies 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, the WP29 considers that only identified reports should be communicated through whistleblowing schemes in order to satisfy this requirement. WP29 holds that whistleblowing schemes should be built in such a way that they do not encourage anonymous reporting as the usual way to make a complaint.

According to section 2 A-4 of the Working Environment Act, when supervisory authorities or other public authorities receive notification concerning censurable conditions, any person who performs work or services for the body receiving such notification shall be obliged to prevent other persons from gaining knowledge of the employee's name or other information identifying the employee. This duty of confidentiality also applies in relation to parties to the case (in connection with notification to public authorities) and their representative. However, it is to be noted that the duty of confidentiality does not apply with regard to the content of the notification, for example, factual data or a summary, if the conditions for access to information pursuant to the Freedom of Information Act or the Public Administration Act are otherwise fulfilled.

## 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)?**

After the incorporation of the GDPR into Norwegian law, a 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 proposed Personal Data Act has a provision regarding the use of fake camera surveillance. According to the proposed section 31, when camera surveillance is in breach with 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 the proposed section 31 is defined in the second paragraph of such section 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.

### 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 interpretation of the GDPR. This, according to the preparatory works to the Personal Data Bill incorporating the GDPR, must be clarified through practice and perhaps through guidance from the supervisory authority.

In the preparatory works to the Personal Data Bill, the Ministry of Justice stated that it is not at present necessary to provide 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.

## 14 Employee Monitoring

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

In connection with the implementation of the GDPR, the Ministry has proposed to adopt specific provisions regarding employee monitoring, pursuant to Article 88 of the GDPR. These provisions will be introduced as regulations to the Working Environment Act, and will be applicable if (i) the monitoring is controlled by the employer and pursued “in the undertaking”, and (ii) the monitoring may be regarded as a control measure pursuant to the Working Environment Act. Monitoring in other circumstances shall be assessed pursuant to the general provisions of the GDPR.

The proposed regulations to the Working Environment Act also contain provisions regarding video surveillance of places in the employer’s undertaking that are frequented by a limited group of persons. Such video surveillance would only be permitted if, due 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. 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.

With regards to examination of employee emails, the Ministry of Justice has proposed that the provisions existing prior to the implementation of the GDPR in Norwegian law should also apply once the GDPR has been implemented. These are likely to be introduced as regulations to the Working Environment Act.

An employer may only explore, open or read email in an employee’s email box (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 term “necessary” aforementioned is interpreted restrictively. These provisions also apply to other personal workspaces and 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 proposed regulations (see question 14.1), the employee shall be notified whenever possible and given an opportunity to speak before the employer makes any such examination as mentioned in question 14.1. In the notice, the employer shall explain why the criteria mentioned above in question 14.1 are believed to be met and 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 as early as possible to discuss needs, designs, implementation and major changes to control measures in the undertaking with the employees’ elected representatives.

See also question 14.2.

## 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 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) expects 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) expects 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 the proposed section 16 of the Personal Data Bill, the duty to notify the data subject does not apply to the extent such notification will reveal information: (i) that is of interest 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 the higher of €10 million or 2% of worldwide turnover.

## 16 Enforcement and Sanctions

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

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
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 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.	N/A
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).	N/A
Authorisation and Advisory Powers	The NDPA 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.	N/A
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 of the preceding financial year, whichever is the higher.	N/A
Non-Compliance With an Order by 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.	N/A

### 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.

As the powers of the data protection authorities will change when GDPR becomes effective, the approach of the NDPA to exercising the powers mentioned above in question 16.1 is currently not certain. However, the NDPA is an active and effective supervisory and educational authority and is expected to continue its important role after the implementation of the GDPR. Note also that the numbers and cases mentioned below are based on the powers of the authority prior to the implementation of the GDPR and not the powers pursuant to the GDPR (described in question 16.1).

In 2017, the NDPA performed 24 supervisions. During 2017, the NDPA received a record high number of cases and case documents. They received 1,807 new cases and in total 3,860 documents. The number of individual decisions is also the highest in many years, being 683. They received 39 complaints and made resolutions on penalties/compulsory fines in 16 cases during 2017. The penalties imposed by the NDPA have ranged from NOK 37,500 to 400,000. The highest infringement penalty was imposed after the NDPA during a local control found that Oslo University Hospital had unlawfully collected and processed health data and biological material. The number of issued licences in 2017 was 183.

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

For the time being, we have not seen any cases where the NDPA has exercised its powers against companies established in other jurisdictions.

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

### 17.1 How do companies 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 probably 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 2017, the NDPA held 417 lectures, which is more than twice as many as in 2016. Due to the preparation for the GDPR, the supervisory activity was significantly reduced in 2017. In 2017, the NDPA also started the work to reduce the amount of cases that are handled pursuant to the Personal Data Act, in order to prioritise external lectures and guidance meetings. In spite of this work, the NDPA, as mentioned above, received a record high number of cases in 2017.

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

The major regulatory change brought by the GDPR has been the most important and substantial task and focus for the NDPA in 2017, including guidance and educational activities.

An especially "hot topic" is the principle of data protection by design. Many businesses have consulted the NDPA in order to better understand this principle, and the authority has prepared several guidance documents on the principles of data protection and especially the principle of data protection by design. The annual report for 2017 of the NDPA pointed out that a special challenge in the future will be that old systems do not meet the principle of data protection by design. The authority has therefore encouraged businesses to plan on phasing out old systems that do not provide sufficient and adequate protection of data. This will in particular be important for organisations in the health sector.

Another "hot topic" is the development of artificial intelligence and robots. In 2017, the Norwegian Parliament passed a new law on the testing of automatically operated vehicles. Such vehicles will be collecting a substantial number of data about passengers and the surroundings. In addition, the Norwegian drone market has extended monitoring from the air considerably.

**Line Coll**

Wikborg Rein Advokatfirma AS  
Dronning Mauds gate 11  
P.O. Box 1513 Vika  
0117 Oslo  
Norway

Tel: +47 22 82 75 97  
Email: lco@wr.no  
URL: www.wr.no/en

Line Coll is a Partner at Wikborg Rein's Oslo office and Head of the firm's Technology and Digitalisation team. Line specialises in privacy and digitalisation, and has more than 20 years' practical experience as a lawyer within data protection law, privacy, the use of new technology and digitalisation, both as a business lawyer for a wide range of public and private Norwegian and international clients, as well as an in-house lawyer at Statoil ASA (Equinor). Line has published books and articles on data protection and privacy, and is a frequent speaker at conferences.

She assists Norwegian and foreign clients in the public as well as private sector, primarily with issues relating to privacy and data protection and e-commerce law.

Within the field of privacy and data protection, she has assisted Norwegian and international clients with GDPR compliance, both strategic advice on risk and approach and practical issues such as drafting of data process agreements, privacy and cookie policies, the review of policies for the setting up of an internal whistleblowing system, and the review and filing of EU standard contractual clauses for transfer of personal data to third countries.

**Vilde Juliussen**

Wikborg Rein Advokatfirma AS  
Olav Kyrres gate 11  
P.O. Box 1233 Sentrum  
5811 Bergen  
Norway

Tel: +47 55 21 52 39  
Email: vjl@wr.no  
URL: www.wr.no/en

Vilde Juliussen is an Associate at Wikborg Rein's Bergen office and is part of the firm's Technology and Digitalisation team. She assists Norwegian and foreign clients in the public as well as private sector, primarily with issues relating to privacy and data protection.

Within the field of privacy and data protection, she has assisted Norwegian and international clients with the preparation for the new EU regulation (GDPR), including the review of data processing agreements, privacy policies, routines and systems.

## WIKBORG | REIN

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, IPR; 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.

# Portugal

Sónia Queiróz Vaz



Cuatrecasas

Ana Costa Teixeira



## 1 Relevant Legislation and Competent Authorities

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

Portugal was regulated by Law 67/98 of 26 October (“Data Protection Act”), which transferred into the Portuguese legal system Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Currently, with the publication of Regulation (EU) 2016/679 of 27 April 2016 (“GDPR”), Law 67/98 will be revoked, with effect from May 2018.

At this moment, the Portuguese Government has presented to Parliament the following proposal of Law 120/XIII, the draft law implementing Regulation (EU) 2016/679 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, approved during the current month in the national legal order.

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

There are a few more laws in Portugal, which impact data protection, for example:

- Constitution of the Portuguese Republic – Article 35 (use of computerised data);
- Act 2/94 of 19 February – establishes the control and verification mechanisms for the Schengen Information System (“SIS”);
- Law 46/2012 of 29 August – transposes the part of Directive 2009/136/EC amending Directive 2002/58/EC of the European Parliament and of the Council of 12 July on the processing of personal data and the protection of privacy in the electronic communications sector, introducing the first amendment to Law 41/2004 of 18 August and the second amendment to Law 7/2004 of 7 January;
- Regulation no. 1093/2016, of 14 December, which regulates the use of drones;
- Decree-Law no. 298/92, of 31 December, General Regime of Credit Institutions and Financial Companies; and
- Law 83/2017 of 18 August, measures to combat money laundering and the financing of terrorism.

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

The Portuguese health, labour, banking and insurance sectors are subject to additional and specific statutory restrictions in relation to data protection due to their sensitive nature.

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

The Data Protection Act has created the *Comissão Nacional de Protecção de Dados* – the Portuguese Data Protection Authority (“CNPD”) – as the empowered body to supervise and monitor the compliance with laws and regulations within the area of personal data protection, with strict respect for human rights and the fundamental freedoms and guarantees enshrined in Portuguese law.

## 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 (“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 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; where the purposes and means of such processing are determined by European Union or Member State law, the controller or the specific criteria for its nomination may be provided for by European Union or Member State law.

## ■ “Processor”

A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

## ■ “Data Subject”

An identifiable person who can be identified, directly or indirectly, in particular with reference to an indication number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

## ■ “Sensitive Personal Data”

A special category 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”

An incident in which sensitive, confidential or otherwise protected data has been accessed and/or disclosed in an unauthorised fashion.

## ■ Other key definitions – please specify (e.g., “Pseudonymous Data”, “Direct Personal Data”, “Indirect Personal Data”)

### ■ “Pseudonymous Data”

The term “Pseudonymous Data” is not used and there is no analogous concept in the Data Protection Act.

### ■ “Direct Personal Data”

The term “Direct Personal Data” is not used and there is no analogous concept in the Data Protection Act.

### ■ “Indirect Personal Data”

The term “Indirect Personal Data” is not used and there is no analogous concept in the Data Protection 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 new Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the European Union, regardless of whether the processing takes place in the European Union or not.

This Regulation applies as well to the processing of personal data of data subjects who are in the European Union by a controller or processor not established in the European Union, 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 European Union; or the monitoring of their behaviour as far as their behaviour takes place within the European Union.

The draft law will apply to the processing of personal data carried out in the national territory, regardless of the public or private nature of the person responsible for the processing, even if the processing of data is carried out in compliance with legal obligations or in the scope of the pursuit of the public interest, with all the exclusions provided for in Article 2 of the RGPD.

This law shall also apply to the processing of personal data carried out outside the national territory when: carried out within the framework of the business of an establishment in the national territory; it affects holders of data living in the national territory, when the activities are subject to Article 3 (2) of the RGPD; or it affects holders of data who, being Portuguese, live abroad and whose data are registered in the consular posts.

## 4 Key Principles

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

#### ■ Transparency

The processing of personal data shall be lawful, fair and processed in a transparent manner in relation to the data subject.

#### ■ Lawful basis for processing

The personal data must be processed lawfully and with respect in the principle of good faith.

#### ■ Purpose limitation

The personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

#### ■ Data minimisation

The personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

#### ■ Proportionality

The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality.

#### ■ Retention

The continued storage of data for compliance, legal obligations or business reasons.

In accordance with the Portuguese Data Protection Authority’s decision, the personal data shall be deleted:

- immediately, when they are revealed to be incorrect or unreasonable;
- within six months from the closing of the investigations, when no disciplinary or judicial proceeding will take place; or
- immediately after the end of the judicial or disciplinary proceeding, under a restricted access information system.

#### ■ Other key principles – please specify

#### ■ Storage limitation

Data should be kept in a form, which 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.

#### ■ Accountability

The controller shall be responsible for, and be able to demonstrate compliance with the principles relating to the processing of personal 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

The data must be available for immediate access, with no excessive costs, by the data subject. Furthermore, the right



of access must be exercised before the Data Controller or, if applicable, the Data Processor.

This right comprises three exceptions:

- a. medical data, including genetic data, whose access must be exercised only by a doctor appointed by the data subject;
- b. police data, whose access is through the CNPD; and
- c. the data for journalistic use and/or artistic or literary purposes, whose access must be performed through the CNPD.

#### ■ **Right to rectification of errors**

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

#### ■ **Right to deletion/right to be forgotten**

The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay.

This right applies where one of the following grounds relates:

- a. the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- b. the data subject withdraws consent on the processing and where there is no other legal ground for the processing;
- c. the data subject objects to the processing and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing;
- d. the personal data have been unlawfully processed;
- e. the personal data have to be erased for compliance with a legal obligation in European Union or Member State law to which the controller is subject; or
- f. the personal data have been collected in relation to the offer of information society services.

#### ■ **Right to object to processing**

The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to the processing of personal data concerning him or her, including profiling based on those provisions.

The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

#### ■ **Right to restrict processing**

The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

- a. the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
- b. the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
- c. the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; or
- d. the data subject has objected to processing pursuant pending the verification whether the legitimate grounds of the controller override those of the data subject.

#### ■ **Right to data portability**

The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

- a. the processing is based on consent or on a contract; and
- b. the processing is carried out by automated means.

#### ■ **Right to withdraw consent**

When the processing is based on data subject consent, the data subject has the right to withdraw his or her consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal.

#### ■ **Right to object to marketing**

The data subject can oppose the processing of his personal data for marketing purposes. In order to do so, it is necessary to send a letter to the company concerned, expressing the right to object to receiving more mail and wait a reasonable time for the company to withdraw his information from the listing of mailings. In cases where the receipt of mail persists from the same company, the data subject should complain to the CNPD.

If the data subject does not wish to receive, in general, this type of mail, it is possible to request that his name and address be included in the designated "Robinson Lists" in charge of the Direct Marketing Association.

With the new Regulation, the data subject continues to have the right to oppose to marketing communications; however, there have been important changes, which, in practice, means that the data subject has to physically confirm that they want to be contacted. The controller needs to guarantee that the data subject has actively given (and not assumed) permission confirming they want to be contacted. Therefore, a pre-ticked box that automatically opts the data subject in will not be acceptable – opt-ins need to be a deliberate choice.

#### ■ **Right to complain to the relevant data protection authority(ies)**

The data subject has the right to lodge a complaint with a supervisory authority. Furthermore, the supervisory authority has to handle the complaints lodged by the data subject, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary.

#### ■ **Other key rights – please specify**

There are no other specific key rights.

## 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?

With Law 67/98, the controller was obliged to notify the CNPD before carrying out any personal data processing operation. With the publication of the new Regulation, this obligation ends.

Directive 95/46/EC provided for a general obligation to notify the processing of personal data to the supervisory authorities. While that obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal

data. In this sense, the European legislator decided to abolish general notification obligations, and replace them with effective procedures and mechanisms, which focus instead on those types of processing operations which are likely to result in a high risk to the rights and freedoms of natural persons by virtue of their nature, scope, context and purposes. Such types of processing operations may be those which in, particular, involve using new technologies, or are of a new kind and where no data protection impact assessment has been carried out before by the controller, or where they become necessary in the light of the time that has elapsed since the initial processing.

Notwithstanding, there are new obligations, for example, the obligation to notify in the case of a personal data breach – the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority. This is, however, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

Prior consultation is also foreseen. The controller shall consult the supervisory authority prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk. It is not a notification procedure, but it is a measure that stems from the legislator's decision to create effective procedures and mechanisms.

---

**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)?**

---

Considering our answer to question 6.1, in the case of data breach, the controller has to notify the supervisory authority and to communicate to the data subject the personal data breach, without undue delay.

---

**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 communication should be done within 72 hours to the supervisory authority and if applicable, it shall be accompanied by reasons for the delay.

In addition and 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.

Such communications to data subjects should be made as soon as reasonably feasible and in close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities, such as law-enforcement authorities.

For example, the need to mitigate an immediate risk of damage would call for prompt communication with data subjects, whereas the need to implement appropriate measures against continuing or similar personal data breaches may justify more time for communication.

---

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

---

The controller's infringement of the obligation to notify the data breach and to do a prior consult to the supervisory authority is subject to administrative fines of up to 10,000,000 EUR, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

---

**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?**

---

Yes, the list of notifications and authorisations made before the entry into force of the changes made by the Regulation is available online, on the CNPD website.

---

**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 controller and the processor shall designate a data protection officer in any case where:

- a. the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
- b. the core activities of the controller or the processor consist of 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
- c. the core activities of the controller or the processor consist of processing on a large scale of special categories of data and personal data relating to criminal convictions and offences.

The appointment of a data protection officer may also be voluntary.

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

Infringements of the following provisions shall be subject to administrative fines of up to 10,000,000 EUR, 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 to his or her role as a Data Protection Officer?**

Data protection officers, whether or not they are an employee of the controller, should be in a position to perform their duties and tasks in an independent manner.

The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.

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

Yes, a group of companies can appoint a single data protection officer, as long as the data protection officer is easily accessible from each facility. Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking into account their organisational structure and size.

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

A data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the following tasks:

- a. to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other European Union or Member State data protection provisions;
- b. to monitor compliance with this Regulation, with other European Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
- c. to provide advice where requested as regards the data protection impact assessment and monitor its performance;

- d. to cooperate with the supervisory authority; and
- e. to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation, and to consult, where appropriate, with regard to any other matter.

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

The data protection officer has to have the ability to fulfil the following tasks:

- a. to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other European Union or Member State data protection provisions;
- b. to monitor compliance with this Regulation, with other European Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
- c. to provide advice where requested as regards the data protection impact assessment and monitor its performance;
- d. to cooperate with the supervisory authority; and
- e. to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation, and to consult, where appropriate, with regard to any other matter.

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

The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.

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

Yes, the data protection officer's contact information must be published 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?**

Yes, processing data by a processor shall be governed by a contract or other legal act under European Union or Member State law that is binding on the processor with regard to the controller and that sets out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.

## **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 should be a contract or other legal act under European Union

or Member State law, and it should be in writing, including in electronic form. The controller and processor may choose to use an individual contract or standard contractual clauses, which are adopted either directly by the Commission or by a supervisory authority in accordance with the consistency mechanism and then adopted by the Commission.

That contract or other legal act shall stipulate, in particular, that the processor:

- a. processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by European Union or Member State law to which the processor is subject;
- b. in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
- c. ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and takes all measures required pursuant to Article 32;
- d. respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;
- e. takes into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;
- f. assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36, taking into account the nature of processing and the information available to the processor;
- g. at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless European Union or Member State law requires storage of the personal data; and
- h. makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute 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?)

Law 41/2004 of 18 August on the protection and processing of personal data in e-communications was amended by Law 46/2012 of 29 August, which transposed Directive 2009/136/EC.

According to the referred law and in relation to individuals, the sending of unrequested communications for direct marketing purposes is subject to the express prior consent of the subscriber or user (that is, the "opt-in" rule applies). This includes the use of automated calling and communication that do not rely on human intervention (automatic call devices), facsimile or electronic mail, including SMS, EMS, MMS and other similar applications. This does not apply to legal entities and, accordingly, unrequested direct marketing communications are allowed. Nevertheless, the "opt-out" rule applies, and legal entities may refuse future communications and enrolment into the non-subscribers' list.

With the new Regulation on data protection, the consent acquires a new relevance, namely in the marketing sector. This means that any organisation that wants to collect data must communicate clearly to the data subject what that data is going to be used for. The data subject will need to give their consent to that use and the consent needs to be clear, "*informed, specific, unambiguous, and revocable*". Data subjects also need to be informed about their right to withdraw consent.

On 20 January, the European Commission made public the proposal for a Regulation on Privacy and Electronic Communications (e-Privacy Regulation) which should replace Directive 2002/58/EC (e-Privacy Directive). The proposal aims to complement the General Regulation on Data Protection (RGPD), and comes with the stated purpose of adapting the current legal framework on privacy to the new technological reality and market development. The new rules cover matters for direct marketing, despite the fact that they do not innovate in relation to the current regime, since the requirement of prior opt-in is maintained for most cases, except in the case of communications concerned with products or services similar to those which the data subject has already acquired, provided, of course, that he is able to oppose such communications, both at the time of collection and at the time of sending each message (opt-out).

### 9.2 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.)

As referred to previously, this is subject to prior express consent of the subscriber who is a natural person, or the user, of the sending of unsolicited communications for direct marketing purposes, namely through the use of automated call and communication systems that are not dependent on human intervention.

Entities that promote the sending of communications for direct marketing purposes, in particular through the use of automated call and communication systems not dependent on human intervention (automatic calling machines), fax machines or electronic mail, including SMS (EMS (enhanced messaging services), MMS (multimedia messaging services) and other similar applications, must have an up-to-date list of persons expressing consent to the reception of such communications, as well as of customers who did not object to their receipt.

It is incumbent upon the Directorate General of Consumers ("DGC") to keep up to date a national list of legal persons that expressly object to the receipt of unsolicited communications for direct marketing purposes. The entities that promote the sending of communications for direct marketing purposes are obliged to consult the list, updated monthly by the DGC, which is available on request.

### 9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

Yes, these obligations apply to marketing sent from other jurisdictions when the representative is established in the EU. The new data protection regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the European Union, regardless of whether the processing takes place in the European Union or not, including the circumstances where the controller or processor are not established in the European Union: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the European Union; or (b) the



monitoring of their behaviour as far as their behaviour takes place within the European Union.

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

Yes, according to our experience, although the CNPD is not very proactive in the execution of its supervision and monitoring powers; following a complaint, the CNPD is very quick in the beginning of the investigations and in the issuance of decisions. This will be improved by the GDPR.

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

With the new data protection rules, the legislator wanted to give the data subject control of their data. One of the most important aspects is, as previously said, the revision of what constitutes personal data and how to obtain consent for its use. The consent requests must be prominent, unbundled from other terms and conditions, concise and easy to understand, and user-friendly, and it must specifically cover the controller's name, the purposes of the processing and the types of processing activity. This means that when the purchase is not transparent and in accordance to the referred demanding, it is unlawful.

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

The CNPD and ICP-ANACOM are empowered to issue fines of up to 5,000,000 EUR and to seize any equipment, devices, or materials used to commit the infraction. Delays in complying with any orders or requests from the CNPD or ICP-ANACOM may also attract a fine of up to 100,000 EUR for each day up to a maximum of 3,000,000 EUR (30 days' delay).

When applicable, according to the Regulation (EU) 2016/679 of 27 April 2016, a fine of up to 20,000,000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher, can be issued.

## **10 Cookies**

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

In accordance with Directive 95/46/EC, legislative restrictions regarding the purposes of cookies or similar devices ensure that users are made aware of information being placed on the terminal equipment they are using. Users should have the opportunity to refuse to have a cookie or similar device stored on their terminal equipment. This is particularly important where users other than the original user have access to the terminal equipment and thereby to any data containing privacy-sensitive information stored on such equipment. Information and the right to refuse may be offered once for the use of various devices to be installed on the user's terminal equipment during the same connection and covering any further use that may be made of those devices during subsequent connections. Access to specific website content may still be made conditional on the well-informed acceptance of a cookie or similar device, if it is used for a legitimate purpose. A new regulation

(E-Privacy Regulation) clarifying the previous regime on cookies incorporates in the recitals or in the applicable provisions some of the interpretations or suggestions previously expressed by the Working Group of Article 29, both in its Document of Work 2/2013 on requirements for obtaining consent, as in Opinion 4/2012 on exemption of consent. The Regulation draft refers that for web browsers to be able to obtain end-users' consent as defined under Regulation (EU) 2016/679, for example, to the storage of third-party tracking cookies, they should, among others, require a clear affirmative action from the end-user of terminal equipment to signify his or her freely given, specific, informed and unambiguous agreement to the storage and access of such cookies in and from the terminal equipment.

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

The E-Privacy law proposal does not distinguish between different kinds of cookies, but it would be better for everyone if it did. Notwithstanding, the actual and still-in-force E-Privacy Directive requires prior informed consent for storage or for access to information stored on a user's terminal equipment. In other words, the users must be asked if they agree to most cookies and similar technologies (e.g., web beacons, Flash cookies, etc.) before the site starts to use them. Some cookies are clearly exempt from consent according to the EU advisory body on data protection WP29, including:

- user-input cookies (session-id) such as first-party cookies to keep track of the user's input when filling online forms, shopping carts, etc., for the duration of a session or persistent cookies limited to a few hours in some cases;
- authentication cookies, to identify the user once he has logged in, for the duration of a session;
- user-centric security cookies, used to detect authentication abuses, for a limited persistent duration;
- multimedia content player cookies, used to store technical data to play back video or audio content, for the duration of a session;
- load-balancing cookies, for the duration of session;
- user-interface customisation cookies such as language or font preferences, for the duration of a session (or slightly longer); and
- third-party social plug-in content-sharing cookies for logged-in members of a social network.

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

To date, the Portuguese Data Protection Authority has not taken any enforcement action in relation to cookies.

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

The CNPD and ICP-ANACOM are empowered to issue fines of up to 5,000,000 EUR and to seize any equipment, devices or materials used to commit the infraction. Delays in complying with any orders or requests from the CNPD or ICP-ANACOM may also attract a fine of up to 100,000 EUR for each day up to a maximum of 3,000,000 EUR (30 days' delay).

## 11 Restrictions on International Data Transfers

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

Without prejudice to the tax or customs decisions of the community, personal data may move freely between Member States of the European Union. In accordance to the GDPR, a transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation. In the absence of a decision pursuant to the controller or the processor, it may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

### 11.2 Please describe the mechanisms companies 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 GDPR, as appropriate, safeguards the transfer of data by companies with the following mechanisms:

- a legally binding and enforceable instrument between public authorities or bodies;
- binding corporate rules;
- standard data protection clauses adopted by the Commission;
- standard data protection clauses adopted by a supervisory authority and approved by the Commission;
- an approved code of conduct, together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or
- an approved certification mechanism, together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

### 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 GDPR has specific requirements regarding the transfer of data out of the European Union. One of the requirements is that the transfer must only occur in countries deemed as having adequate data protection laws. The Commission has to decide if the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. In addition, such transfer shall not require any specific authorisation, except the adequate level of protection.

When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:

- the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;
- the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and
- the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

## 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 CNPD has issued Decision 765/2009 on the principles applicable to the processing of personal data for the purposes of internal communication of irregular management and financial acts (whistle-blower hotlines).

The Portuguese Data Protection Authority has considered that the legitimate purpose in this matter is the management of whistle-blowing of irregular acts, in order to prevent and/or repress irregularities such as corruption, banking and financial crime and matters affecting accounts, internal account controls and auditing.

In order to obtain the mandatory prior authorisation for processing, the Data Controller must prove that it is necessary for the execution of legitimate purposes, provided that no fundamental rights of the data subject prevail. The Data Controller must be individually identified, and the Portuguese Data Protection Authority will only admit Co-Controllers where there is a case of absolute impossibility to determine individually the responsibility for processing. The Data Controller is, therefore, considered as the company which adopts internal procedures and ensures means that allow the whistle-blowing and subsequent investigations of behaviours contrary to the law or company's policies, and ultimately decide if the complaint will be sent for disciplinary or judicial proceeding. Hence, the Data Controller must establish the rules applicable to the communication and processing of complaints, appointing those people or bodies which are especially responsible for the collection and processing of complaints – they must be in a limited number, with technical education and subject to strict confidentiality obligations contracted. The Data Processor, if any, must assume, by means of contract, the liability of not using the data for other purposes than those authorised, to guarantee the confidentiality of data, respect the deadline for its preservation and record, and to destroy all physical

or electronic records of personal data in the term of the contract with the Data Controller. Nonetheless, the Data Controller is still bound by an obligation of result regarding the protection of quality or safety of personal data. In this matter, the company must ensure that an agreement in the above conditions is entered into with the Data Processor (contractor), if that is the case.

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

Anonymous whistle-blowers are not allowed by the Portuguese Data Protection Authority, so as to prevent the risks of slanderous complaints and discrimination. Instead, a confidentiality regime should be adopted by the Data Controller.

## **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)?**

As explained before, these notifications took place before the entry into force of the Regulation.

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

Yes, only for the purpose of protection of persons and property.

## **14 Employee Monitoring**

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

According to the Recommendations of the Portuguese Data Protection Authority regarding the monitoring of employees in the workplace, the monitoring of phone calls, email and internet access is permitted as follows:

#### **a. Phone calls**

The employer shall define with accuracy the level of tolerance regarding the use of telephones and the forms of control adopted. However, one should not think, in a simple manner, that employees could be prevented from responding to needs which are strictly private and which correspond to the way our society is structured.

In cases where monitoring of phone calls takes place, other data than that which is strictly necessary to achieve the purpose of the control shall not be processed. The processing shall be limited to the user identification, his rank/function in the corporation, the number called, the type of call (local, regional or international), the continuance of the call and the cost.

The undue access to communications, the use of any tapping device, storage, interception and surveillance of the communications by the employer is forbidden.

In the cases foreseen by law that require the recording of phone calls, in order to document a business declaration and prove its validity and efficacy, this "interception" can only occur with the prior consent of the users, or legal provision.

#### **b. Use of email and internet access**

The employer shall set up clear and precise rules on the use of the email and internet access for private purposes, which shall be based on the principles of adequacy, proportionality, mutual collaboration and reciprocal trust.

These rules shall be submitted to the opinion of the employees and their representatives, being expressly publicised, in order to ensure good information about the level of tolerance and about the consequences of non-compliance with the rules.

It is advisable that the employer allows the employees to use, in moderate and reasonable terms, the new technological means made available to them.

The system administrator is bound by the obligation of professional secrecy and cannot disclose to third parties the employees' private information that comes to his knowledge within the scope of monitoring.

#### **c. Specific principles for the use of email**

Even in the case of the employer prohibiting the use of emails for private purposes, this does not automatically give the employer the right to open the emails addressed to the employee.

The monitoring powers of the employer shall be made compatible with the rights of the employees, in order to ensure that intrusions can be avoided. The employer shall therefore choose non-intrusive control methods, according to the principles previously defined and being of the employees' knowledge.

The employer shall not undertake a permanent and systematic monitoring of the employees' email. The control shall be punctual and towards the areas or activities that present a greater "risk" for the business.

The specific professional secrecy for some employees (i.e., medical secrecy or protection of the sources in journalism) shall be preserved.

The level of exigency and accuracy in relation to the monitoring of received and sent emails should be clearly distinctive. Also, the reasons for opening the inbox of the employee in the case of a long absence (holidays or illness) shall be clearly expressed and completed with the employee's prior knowledge.

The monitoring of emails shall aim principally to guarantee the security of the system and its performance. The employer may also adopt the necessary procedures – always with the knowledge of the employees – to filter certain files that may not be professional emails (.exe files, mp3 or image files). The detection of a virus does not justify the reading of the emails received.

Eventual monitoring for prevention or detection of commercial secrets disclosure shall be directed exclusively for the employees with access to those secrets and only when there are strong suspicions.

Access to the employee's email shall be the last recourse to be used by the employer, and it should be done in the presence of the employee concerned. The access should be limited to watching the addresses of the recipients, the subject, the date and hour. The employee – if this is the case – may specify the existence of emails of a private nature and object to their reading by the employer. In the face of this opposition, the employer shall refrain from viewing the content of the email.

#### **d. Principles on internet access**

A certain level of tolerance should be admitted in relation to internet access for private purposes, particularly if it occurs out of working hours.

The employer shall not undertake a permanent and systematic control of internet access. It shall be done in a global way, not individualised, in relation to all access inside the corporation, with

reference to the time of the web connection. It is admissible that the employer processes data about the most acceded websites, but without identifying the place of origin of the access.

Whenever there are reasons of costs and productivity involved, the monitoring shall be done through the counting of the time of connection, independently of the sites visited. If excessive and disproportionate use is verified, the employee shall be warned in respect to his level of use. The control of the time spent daily on the internet and the websites consulted by the employee shall only occur in exceptional circumstances; in particular, when the employee, after the warning, doubts the employer's indications and wishes to confirm such accesses.

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

Regarding the WP29 guidelines on consent, it is well noted that there are situations where a data subject will not have a real choice because of an imbalance of power in their relationship with the controller (e.g., between an employer and employee, or citizen and public authority). This is reasonably well understood and means employers should, by default, avoid reliance on consent as a lawful basis for processing.

In this way, and considering the WP29 understanding, the employers should rely on other basis for the performance and process of data; for instance, the contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract, or when the processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security.

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

The level of use of the corporation means, for private purposes, the delimitation of the conditions for the data processing and the definition of the forms of monitoring adopted shall be included in internal Rules of Procedure, which shall be submitted to the workers, council and approved by the Labour Inspection Board.

The employer shall publicise the content of the Rules of Procedure; namely, by posting it in the corporation's headquarters and in all other workplaces, in order to allow the employees to obtain full knowledge of it.

## 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, there is. The GDPR states that there should be preventive safeguards, security measures and mechanisms to mitigate the risk of data breach. The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

#### 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) expects voluntary breach reporting.

Yes, please see the answers to section 6.

#### 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) expects voluntary breach reporting.

Yes, please see the answers to section 6.

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

The GDPR provides for the infringement of the obligation to notify in case of data breach and for the obligation to apply appropriate technical and organisational measures to ensure data security, fines up to 10,000,000 EUR or, in the case of a company, up to 2% of the total worldwide annual turnover of the previous financial year, whichever is the higher.

## 16 Enforcement and Sanctions

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

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
Power to supervise and monitor compliance with the laws and regulations in the area of personal data.	Deliberating on the application of fines (administrative sanctions).	Not applicable.
Investigative powers which may have access to data undergoing processing and powers to collect all the information necessary for the performance of its supervisory duties.		

#### 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. No court order is required.

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

The CNPD was not a proactive entity until the current date so there are no recent cases to report in Portugal regarding the exercise of



power. According to our experience, although the CNPD is not very proactive in the execution of its supervision and monitoring powers, following a complaint, the CNPD is quick in the beginning of the investigations and in the issuance of decisions. Also, the CNPD is very strict in the interpretation of the personal data protection laws and regulations and in the protection of data subjects' rights.

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

We are not aware of any cases.

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

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

According to our experience, Portuguese companies typically respond that they are subject to European Union personal data protection obligations, namely those regarding confidentiality and the impossibility to share data without legitimate grounds. In Portugal, there is a conflict between the data protection law and e-discovery demands, which is strengthened by the differences between the different judicial systems. In Portugal, this issue is only raised in big group companies. In these cases, the reply to foreign e-discovery requests is always limited by the compliance with Portuguese laws and regulations on data protection.

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

Although the CNPD has not furnished any specific guidelines on this issue, the implications of e-discovery exercises are relatively easy to identify:

- Furnishing adequate notice to affected Portuguese individuals.
- Ensuring the underlying legitimacy of the collection and processing (and, frequently, international transfer) of personal data.
- Maintaining appropriate limitations or controls on the scope of the data collection exercises.
- Abiding by international data transfer rules.

### **18 Trends and Developments**

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

##### **The Judgment of the European Court of Human Rights (Third Section), 2018-01-09, Procedure 1874/13**

The European Court of Human Rights ("ECHR") was called upon to rule on a dispute, dating back to 2009, regarding the dismissal

of five employees of a Spanish supermarket which had been filmed through the surveillance system installed therein to register possible thefts, following the verification of losses in the previous months that ranged between 7,000 EUR and 25,000 EUR.

The Spanish Court of First Instance, in two separate judgments, accepted these recordings as evidence, stating that the employer had legitimacy to install visible and hidden surveillance cameras, even though the supermarket's employees only knew of the former and that the purpose of the latter was only to monitor their behaviour. As a basis for its decisions, this court stated that the employer, under Spanish labour law, had legal grounds to monitor and control the worker's compliance with their employment duties, provided that human dignity was not at stake, being the employer the one to assess if this requirement was being fulfilled or not. These decisions were confirmed by the Superior Court of Justice of Catalonia, and the "amparo" appeal to the Constitutional Court was considered inadmissible.

On 9 January 2018, the ECHR considered that the system of video surveillance and subsequent recordings of the employees constituted a violation of Article 8 of the European Convention on Human Rights, which enshrines the right to respect private and family life. Even if the installation of the hidden camera surveillance system came about as a result of a suspicion of the behaviour of the employees, it was not limited to a particular person or group but had implications for all the workforce and for a large period of time, thus being a disproportionate measure to the defence of the property right at risk. In accordance with the Spanish Personal Data Protection Law, this data collection was limited by an obligation to inform the data subjects in an explicit, precise and unambiguous manner, which has not been fulfilled. The ECHR considered that the national proceedings were, in their entirety, fair, since the evidence was not limited to the unlawfully recorded images and that the dismissed employees were given a fair trial, also stating that it was not up to this court to judge the facts as an appeal court. Nevertheless, this court pointed out that the infringement of Article 8 of the European Convention on Human Rights caused moral damages to the five Spanish citizens, condemning the Spanish state to indemnify each of them on the amount of 4,000 EUR, plus costs and expenses incurred before the national courts.

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

The following "hot topics" are currently a focus for the data protection regulator:

- The national implementation of the Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("General Data Protection Regulation").
- Video surveillance using drones.
- Control of the use of information technologies in the workplace.

**Sónia Queiróz Vaz**

Cuatrecasas  
Praça Marquês de Pombal, nº 2  
1250-160 Lisboa  
Portugal

Tel: +351 21 355 38 00  
Email: [sonia.queiroz.vaz@cuatrecasas.com](mailto:sonia.queiroz.vaz@cuatrecasas.com)  
URL: [www.cuatrecasas.com](http://www.cuatrecasas.com)

Having joined Cuatrecasas in 2008, Sónia Queiróz Vaz is now a Senior Associate coordinating the firm's Intellectual Property, Media and Data Protection department in Portugal.

Sónia has advised on projects involving the evaluation and verification of compliance with obligations relating to personal data and privacy protection, has even helped map how personally identifiable information is processed, and defined strategies for implementing the requirements of the General Regulation on Data Protection.

She is experienced in drafting and negotiating agreements for the exploitation of intellectual property rights (particularly, licensing and transfer rights) in many fields (including broadcasting, publishing and merchandising). She also has extensive expertise in the commercial exploitation of software and audiovisual products domestically and internationally.

She has also provided legal advice on projects concerning consumer rights, industrial property rights, advertising rights and social communication rights.

She has been a member of the Portuguese Bar since 2000.

- 3<sup>rd</sup> Consumer Law and Alternative Consumer Dispute Resolution Course, Universidade Nova de Lisboa, 2016.
- Information Technology Course, Instituto Nacional da Propriedade Industrial, Lisbon, 2016.
- Course on IP and Competition Law, Católica Global School of Law, 2016.
- Post-graduate Course in Information Society Law, Universidade Nova de Lisboa Law School, 2001.
- Law Degree from the University of Lisbon Law School, 2000.

**Ana Costa Teixeira**

Cuatrecasas  
Praça Marquês de Pombal, nº 2  
1250-160 Lisboa  
Portugal

Tel: +351 21 355 38 00  
Email: [ana.costa.teixeira@cuatrecasas.com](mailto:ana.costa.teixeira@cuatrecasas.com)  
URL: [www.cuatrecasas.com](http://www.cuatrecasas.com)

Ana Costa Teixeira has been an Associate Lawyer at Cuatrecasas since 2008.

Ana focuses her practice on the areas of intellectual property, advertising and media law, new technologies law (computer law) and data protection law, providing advice, in particular, on conflicts relating to intellectual and industrial property rights, unfair competition and advertising, as well as with regards to distribution and licence agreements.

Previously, she worked at Almeida Sampaio & Associados.

She has been a member of the Portuguese Bar Association since 2002.

She has also been a teacher at IADE, on the subject of Legal Protection of Trademarks and Branding and Trademark Management (Post-graduate Course), since 2011.

- Law Degree, University of Lisbon Law School, 2002.
- Post-graduate Course in Administrative Litigation, School of Law of the Catholic University, 2006.
- Summer Course on Industrial Property, University of Lisbon Law School, 2008.



Cuatrecasas is a leading Iberian law firm with its main offices in Portugal and Spain and international presence in 10 other countries. We have nearly 1,000 lawyers in 27 offices worldwide, organised by legal practice areas and multidisciplinary teams with expertise in specific commercial and industrial sectors. In Portugal, we have offices in Lisbon and Porto and a total of over 140 lawyers.

Different regions become connected through the firm's client-tailored model that offers the best team for each particular case, depending on the jurisdiction, speciality area and complexity required.

Sixteen offices on the Iberian Peninsula coordinate with the firm's teams in Bogotá, Brussels, Casablanca, London, Luanda, Maputo, Mexico City, New York, São Paulo and Shanghai, thus optimising efficiency of resources and client proximity, and benefiting from the different time zones. The international desks (covering Africa, Latin America, China, France, Germanic countries and the Middle East) and over 20 country-specific groups guarantee the comprehensive approach of the legal advice from Spain and Portugal.

In continental Europe, Cuatrecasas has developed a non-exclusive network with three other leading law firms – Chiomenti in Italy, Gide in France and Gleiss Lutz in Germany – allowing it to offer clients an integrated service in complex cross-border transactions.

# Romania

Pachiu & Associates

Mihaela Cracea



Alexandru Lefter



## 1 Relevant Legislation and Competent Authorities

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

In Romania, the core legal framework for the protection of personal data is set forth by Law No. 677/2001 on the protection of individuals with regard to the processing of personal data and on free movement of such data ("Personal Data Law").

The Personal Data Law implements into the national legal system the provisions of the Directive of the European Parliament and Council No. 95/46 on the protection of individuals, with regard to the processing of personal data and on free movement of such data ("Personal Data Directive").

The scope of the Personal Data Law is to secure and protect the fundamental rights of individuals, mainly the right to intimate family and private life, in connection with the processing of personal data.

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

The minimum security requirements for the processing of personal data are set forth in the Order of the Romanian Ombudsman No. 52/2002 ("Order 52/2002"). The local data protection authority has also issued several decisions with respect to specific aspects of personal data processing.

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

Law No. 506/2004 on personal data processing in the field of electronic communications sets forth the general conditions for processing of personal data in the electronic communications field ("Law 506/2004") and applies to providers of public communication networks and electronic communication services, as well as to providers of subscriber records which, within their economic activities, are processing personal data.

Law No. 238/2009 on the regulation of personal data processing undertaken by the structures/units of the Ministry of Internal Affairs pertaining to activities for prevention, investigation and the fight against criminal activities, as well as for maintenance and assurance of public order, as subsequently republished, sets forth a set of rules for automatic and non-automatic personal data processing in connection to such activities. This law is not applicable to personal data processing and transfers in the field of national defence and security.

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

Romania has set forth a special and independent supervisory and regulatory institution in the field of personal data protection, i.e., the National Supervisory Authority for Personal Data Processing ("ANSPDCP").

ANSPDCP supervises and controls the lawfulness of personal data processing in Romania. For this purpose, ANSPDCP has attributes, such as the ability to receive and assess notifications on data processing, to authorise personal data processing when required by law, to investigate and sanction unlawful processing, and to keep a record of personal data processing, etc.

## 2 Definitions

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

#### ■ "Personal Data"

Any information regarding an identified or identifiable individual. An indefinable individual is deemed to be an individual who can be identified, directly or indirectly, particularly with reference to an identification number or by one or more features pertaining to his physical, physiological, psychical, economic, cultural or social identity.

#### ■ "Processing"

Any operations or set of operations with personal data, by automatic or non-automatic media, such as collecting, registration, classification, storage, adaptation or alteration, extraction, consultation, use, disclosure to third parties by transmission, dissemination or in any other way, annexation or combination, blocking, erasure or destruction.

#### ■ "Controller"

Any individual or private or public legal entity, including central/local public authorities or institutions, who sets forth the purpose and media for the processing of personal data; if the purpose and media of personal data processing are set forth by law, the "controller" shall be deemed as the individual or private or public entity so qualified by the respective law or based on such a law.

#### ■ "Processor"

Any public or private, natural or legal person, including public authorities, agencies and local structures of such, which process personal data on behalf of the controller.

## ■ “Data Subject”

The individual whose personal data are subject to processing by the controller or the processor.

## ■ “Sensitive Personal Data”

Under the Personal Data Law, the concept of “sensitive personal data” is not expressly defined. However, specific categories of personal data, namely those pertaining to racial or ethnic origin, health condition, sexual life, identification details, criminal convictions and minor offences are granted a special legal regime. Furthermore, for the application of such legal provisions, in the standard notification form approved by the decision of the Romanian Personal Data Authority, the following data are qualified as “special personal data”: data denoting the racial origin of data subjects; data denoting the ethnic origin of data subjects; data on the political, philosophical and religious beliefs of data subjects; data on memberships of trade unions, political parties and religious organisations of data subjects; personal identification number; series and number of identification documents; health status; genetic data; biometric data; data regarding sexual life; data regarding perpetration of criminal offences; data on criminal convictions/security measures; data on disciplinary sanctions; data on contraventions; and data in criminal records.

## ■ “Data Breach”

There is no definition of data breach.

## ■ Other key definitions – please specify (e.g., “Pseudonymous Data”, “Direct Personal Data”, “Indirect Personal Data”)

### ■ “Data Recipient”

Any public or private, natural or legal person, including central/local public authorities and agencies, to whom data are disclosed, irrespective of whether such a person is a third party or not. Public authorities to which data are disclosed in connection to their special investigation attributions are not deemed as “data recipients” under the Personal Data Law.

### ■ “Third Party”

Any public or private, natural or legal person, including public authorities, agencies and local structures of such, other than the data subject, the controller, the processor or persons under the direct control of the controller or the processor, who is authorised to process data.

### ■ “Anonymous Data”

Data which, due to their origin or specific processing modality, cannot be associated with an identified or identifiable person.

### ■ “Data Record System”

Any organised data structure, accessed based on determined criteria, irrespective of whether this structure is organised in a centralised or decentralised way or is assigned based on functional or geographic criteria.

## 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 data protection laws apply as well to any processing performed by businesses established in other jurisdictions by using processing means located on Romanian territory, except for in cases where such means are used only for allowing the data to transit the Romanian territory.

## 4 Key Principles

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

#### ■ Transparency

If personal data are obtained directly from the data subject, the controller must disclose at least the following information: the controller’s identity; the purpose of processing; recipients; whether disclosure of all requested data is mandatory; the consequences if the data subject refuses to provide such data; the rights of the data subjects in connection to the proposed processing and effective modalities for the exercise of such rights; and any other information imposed by ANSPDCP depending on the nature of the processing.

If personal data are not obtained directly from data subjects, the controller should provide the information above either before processing or, at the latest, when personal data are disclosed to third parties.

#### ■ Lawful basis for processing

Under the Personal Data Law, personal data shall be processed fairly and lawfully. This is another term that the Personal Data Law does not define. However, “lawful” refers not only to compliance with the Personal Data Law, but also to all other provisions in the Romanian legal system, whether criminal or civil.

#### ■ Purpose limitation

Under the Personal Data Law, personal data can only be collected for specific, precise and legitimate purposes. Subsequent processing of personal data for statistical, historical or scientific research shall not be deemed a breach of the initial purpose if made in accordance to the law, including with the legal provisions of the obligation to notify ANSPDCP.

#### ■ Data minimisation

Under the Personal Data Law, personal data should be adequate, relevant and not excessive in relation to the purpose for which they are processed.

In practice, controllers must ensure that personal data are sufficient for the purpose of processing and that they do not hold more information than they actually need for that purpose.

#### ■ Proportionality

The measure adopted, i.e., the interference with the fundamental right to personal data protection, must also be proportionate to the purpose of processing. This principle is, essentially, about reaching an acceptable compromise between two constitutional values: the fundamental right to personal data protection, which will be restricted; and the legitimate purpose it is aiming to achieve. Interference is in compliance with the principle of proportionality when the processing is balanced, and results in more benefits and advantages to general interest than harm to other conflicting values.

#### ■ Retention

Under the Personal Data Law, personal data, processed for any purpose, cannot be kept for longer than actually necessary for the purpose of processing.

#### ■ Other key principles – please specify

As a general rule, any personal data processing can be made only upon manifest and unequivocal consent of the data subject, save when otherwise provided by law. The consent of the data subject is not required if processing is necessary, *inter alia*: for the execution of an agreement to which the data subject is a party; for taking appropriate actions for the



safeguarding of the life, physical integrity or health of the data subject or another individual; for compliance by the controller with a legal obligation; or for a legitimate interest of the controller or of the third party.

Moreover, for special categories of personal data, processing can be made only upon manifest consent of the data subject, or if absolutely necessary for compliance with a legal obligation of the controller/safeguard of a public interest or of the rights and freedoms of the data subject or other individuals, or if expressly provided by 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**
  - Under the Personal Data Law, any data subject is entitled to request and obtain from the controller confirmation on whether his personal data are subject to processing. The controller must disclose to the applicant, at least, the following information:
    - the purpose of processing, categories of processed data and data recipients;
    - any information regarding the origin of the processed data;
    - the mechanism by which any automatic processing of data is made;
    - information on the conditions for the exercise of the right of intervention over the data and of the right to object to processing; and
    - the possibility to verify the processing in the ANSPDCP Record, to file a complaint against the decisions of the controller with ANSPDCP or with the competent courts of law.
- **Right to rectification of errors**

Any data subject is entitled to request to the controller, at no cost, to adjust or update the personal data.
- **Right to deletion/right to be forgotten**

Any data subject is entitled to request to the controller, at no cost, the following:

  - the erasure or transformation of anonymous data of the personal data subject to unlawful processing; and
  - the notification to third parties to which personal data have been disclosed of any of the operations above, provided that such notification is not impossible and does not entail a disproportionate effort with respect to the legitimate interest that might be violated.
- **Right to object to processing**

Data subjects are entitled to object, at any time, to the processing of their personal data, provided that the grounds of such an objection are sound and legitimate.
- **Right to restrict processing**

Data subjects are entitled to require the blocking of data, at any time, to processing of their personal data, provided that the grounds of such an objection are sound and legitimate.
- **Right to data portability**

Such right shall be available starting from May 25<sup>th</sup> 2018 when the GDPR shall become applicable.
- **Right to withdraw consent**

Under the current legislation, such right is somewhat treated as the right to oppose to processing but starting from May 25<sup>th</sup> 2018, it shall become a distinct right of the data subjects.

### ■ **Right to object to marketing**

Data subjects are entitled to object, at any time, with no cost and without motivation, to any processing of their personal data for direct marketing purposes, as well as to any disclosure to third parties for such purposes.

### ■ **Right to complain to the relevant data protection authority(ies)**

Data subjects can file complaints to ANSPDCP in connection with alleged violations of their rights, as granted by the Personal Data Law. A complaint to ANSPDCP can be filed only upon a lapse of 15 days from the date of registration of a similar complaint with the controller.

If the complaint is found to be grounded, ANSPDCP can decide to temporarily suspend or cease personal data processing, as well as to erase, totally or partially, the personal data which are subject to such unlawful processing. Moreover, ANSPDCP can inform the criminal investigation bodies and file a lawsuit with the relevant courts of law.

*Other key rights – please specify*

### ■ **The right of not being subject to an individual decision**

Data subjects have the right to request and to obtain: (i) the withdrawal or annulment of any decision exclusively taken in consideration of personal data processing by automatic means and which is aimed at assessing features of the data subjects' personality, such as professional capabilities, credibility and behaviour; and (ii) the reassessment of any decision taken in the above-mentioned conditions.

Provided that all the other guarantees are observed, the data subjects can be subject to an individual decision, as mentioned above, if the decision is taken in relation to the execution of an agreement or the decision is authorised by a legal provision.

## 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?

Notification is not required, except for the following cases when notification to ANSPDCP is mandatory:

- processing of personal data related to the racial or ethnic origin of data subjects, data on the political, philosophical and religious beliefs of data subjects, data on memberships of trade unions, and data regarding health status and sexual life;
- genetic and biometric personal data processing;
- processing of data which allows, directly or indirectly, the geographical localisation of natural persons through electronic communication devices;
- processing of data regarding perpetration of criminal offences by the data subject or data regarding criminal convictions, preventive measures, administrative penalties or data on minor offences applicable to the person, performed by private entities;
- personal data processing via electronic devices within an evidence system, aiming to monitor and/or evaluate aspects such as personality, professional competence, credibility, behaviour and other similar aspects;
- processing of personal data by electronic means within evidence systems aiming to take automatic individual decisions relating to the evaluation of solvability, financial and economic situations, actions which may imply disciplinary, minor offences or criminal liability of natural persons by private law entities;

- processing personal data related to ethnic or racial origins, political, religious, philosophical or other similar beliefs, union affiliation, data regarding health status or sexual life performed by associations, foundations or any other non-profit organisations with regard to their members, if the personal data are disclosed to third parties without the prior consent of the data subject;
- processing infants' personal data, if such activity was performed during direct marketing activities, via the internet or electronic messages; and
- personal data processing via video surveillance systems, including the transfer of such data to a non-EU state; such notification shall not be required for cases in which the personal data processing is performed by an individual on his own personal interest, even if the images saved also comprise public domain pictures.

Furthermore, for international transfers of personal data, notification to ANSPDCP is also required, save for cases when such transfers are made based on a special law or international treaty ratified by Romania, or they are implemented exclusively for literary or journalistic purposes when data were already manifestly made available to the public by the data subject, or the data are strictly linked to the data subject being a public person, or taking into account the public nature of that particular person.

---

**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 should be related to each purpose of processing. The businesses are required to provide the ANSPDCP with information as provided under question 6.5 below.

---

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

---

Under the Romanian Data Protection Law, notifications are made based on the purpose 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)?**

---

The data protection authority must be notified by the following: (i) local legal entities; (ii) Romanian subsidiaries of foreign entities (exemptions under question 6.4 are also applicable); and (iii) foreign legal entities, if they are processing personal data by means of any nature located in Romania, save when such means are used exclusively as data transit facilities.

Processing by Romanian representative offices or branches of foreign entities is subject to notification in Romania.

The aspects mentioned under question 6.1 are applicable to all cases listed herein.

---

**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)?**

---

Under the Personal Data Law, the notification must include at least the following:

- a. identification of the controller;
- b. purpose/related purposes of processing;
- c. categories of data subjects;
- d. categories of data recipients;
- e. guarantees pertaining to third-party disclosure;
- f. means by which data subjects are informed of the processing and their rights in connection thereof; estimated date for termination of the processing and subsequent destination of the processed data;
- g. intended transfers abroad (if applicable);
- h. description of the measures implemented for security of the personal data; and
- i. description of any record of personal data related to the processing, as well as on potential links with other personal data processing or records, irrespective of whether such are made/located in Romania.

In the case of international transfer of personal data, the notification will also list the transferred personal data, as well as the destination country for each category of transferred data.

---

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

---

Failure to notify ANSPDCP when mandatory under the Personal Data Law is sanctioned with an administrative fine amounting to between approximately EUR 1,000 and EUR 5,000 (in national currency equivalent), save when incriminated as a criminal offence. Additionally, ANSPDCP may order the temporary or permanent ceasing of the unlawful processing, as well as deletion of the processed data.

---

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

---

No fees are required.

---

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

---

There is no general requirement with respect to the notifications renewal. The notifications should be updated each time changes occur as per the processed personal data, the data subjects, the data recipients, and the means and modalities of processing. In cases where personal data are processed for a different purpose, a separate notification must be filed.

---

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

---

The transfer of personal data to countries which are not deemed to grant an adequate level of protection cannot be made unless authorised by ANSPDCP. The authorisation is not required: if the transfer is made exclusively for journalism, or a literary or artistic purpose; if data have been already disclosed to the public by the data

subject; or if the data are strictly related to the public nature of the activities of the data subject.

In all cases, transfer of personal data to entities located outside Romania can be made only upon prior notification to ANSPDCP.

International transfer is always allowed, among other circumstances, when the data subject has expressly consented to such transfer.

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

Yes. There is only an online notification available.

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

Yes. On the ANSPDCP website, any interested person may search for the notifications submitted by a business.

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

Filling in the online notification might take about two hours. However, in 30 days as of the online filing, the first page of the notification, in hard copy, signed and stamped by the legal representative of the controller, must be registered with ANSPDCP. Failure to register this first page shall result in the refusal of ANSPDCP to consider the notification filed online. As a general rule, the authorisation must be issued in 30 days as of the registration of the relevant notification with ANSPDCP (final version, including all amendments, supplementation and clarifications required by ANSPDCP).

### 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 Personal Data Law does not require the appointment of a Data Protection Officer ("DPO"). Romanian companies do not usually appoint DPOs. However, there is a practice for multinational companies with subsidiaries in Romania to appoint, at parent company level, an employee with duties related to the processing of personal data performed by Romanian subsidiaries.

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

Currently, this is not applicable.

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

Currently, this is not applicable.

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

Currently, this is not applicable.

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

Currently, this is not applicable.

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

In practice, the responsibilities of DPOs focus mainly on advising companies on data protection rights and obligations, and supervising activities related to processing, appropriate notification, management and avoidance of breaches.

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

Currently, no registration formalities are needed.

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

Currently, no registration formalities are needed.

### 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. Any processing of personal data through processors should be made based on a contract.

#### 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 should be in writing, signed by the parties' representatives and should comprise the obligation of the processor to act in accordance with the controller's instructions, as well as the fact that all obligations with respect to the implementation of appropriate organisational and technical measures will be incumbent to it, as well.

### 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?)

Unless the subscriber has given his express prior consent, the following deeds are forbidden:

- marketing communications sent by email; and
- commercial communications made through automatic systems that do not require the intervention of a human operator – by fax, email, SMS or any other method using electronic communication systems destined for the public.

Commercial e-communications should observe the following requirements:

- clear identification of their commercial nature;
- clear identification of the individual or legal entity on behalf of which the communications are made;
- clear identification of promotional offers and of all relevant conditions in connection therewith; and
- clear identification of competitions and promotional games, and the relevant participation conditions must be clearly identifiable.

An exemption from the opt-in mechanism requirement applies when the controller has obtained the consumer's email address on entering a contractual relationship for the trade of specific products or services. Nevertheless, it is only permitted to send emails for the purposes of direct marketing for similar products and services, and in compliance with the opt-out requirements.

**9.2 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.)**

Although not expressly regulated, it is recommended that the data subject is informed, at the beginning of the phone call conversation, of the purpose of such call and the data subject is given the opportunity to stop the conversation.

In what concerns the opt-out register, there is no legal requirement for companies to screen against a "do not contact" list or registry. However, companies have to obtain the express prior consent of the subscriber in order to send commercial communications and the consumer has the possibility to opt-out from receiving these communications in cases where he has not initially objected, but later changes his mind. In such cases, companies should draft a "do not contact" list, including consumers who have exercised their right to opt-out. The list should be considered by the company upon every commercial communication sent to consumers.

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

Considering that local legal provisions apply to any processing performed by a business located in other jurisdictions, but only when it is using local means for such processing, the Romanian legislation shall apply only in case the way the marketing is addressed to data subjects might be construed as a local means of processing.

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

ANSPDCP is one of the authorities with jurisdiction to enforce breaches of marketing restrictions. Additionally, under Law No. 506/2004, the National Authority for Management and Regulation in Communications ("ANCOM") has specific attributes regarding the activity of electronic communication services and communication networks providers.

ANSPDCP has performed a significant number of investigations concerning the processing of personal data and privacy in the field of e-commerce.

Subject to findings regarding unsolicited commercial communications, most of the collectors were sanctioned for lack of expressed prior consent of the subscribers and for failing to tell subscribers that they may reject marketing communications in the future.

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

Although not very widespread, there is a practice in purchasing marketing lists which are of two categories: lists that comprise contact data of individuals; and lists which contain business contact data which may be found on public registers (e.g. Company House). In the majority of the cases, purchasing is not a lawful practice as there is no consent from the data subjects, as their data is to be provided to third parties for marketing purposes.

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

Breach of the legal requirements for marketing communications is sanctioned with administrative fines ranging between approximately EUR 1,100 and approximately EUR 22,000 (in national currency equivalent). Furthermore, for companies with a turnover exceeding the national currency equivalent of EUR 1.11 million, fines can reach up to 2% of the turnover.

Moreover, ANSPDCP may order the temporary or permanent cessation of the unlawful processing, or deletion of processed data.

## 10 Cookies

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

There are no legislative restrictions on using cookies.

**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 Romania.

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

Controllers were mainly sanctioned for failure to obtain the prior consent of data subjects and for failure to provide an appropriate information notice. Furthermore, processing activities were suspended or even ceased, and deletion of the processed data was ordered.

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

Failure to comply with the legal restrictions is sanctioned with administrative fines ranging between approximately EUR 1,100 and approximately EUR 22,000 (in national currency equivalent). For companies with a turnover exceeding the national currency equivalent of approximately EUR 1.11 million, the amount of the fines can reach up to 2% of turnover.

In addition, ANSPDCP may order the temporary or permanent cessation of the unlawful processing.



## 11 Restrictions on International Data Transfers

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

The Personal Data Law sets forth a different set of rules depending on whether the data importer is located in states which are offering an adequate data protection level or not:

#### a. **International transfer to states that offer an adequate level of personal data protection**

Importers in EU and EEA Member States or other states mentioned in the relevant decisions of the European Commission are deemed as granting an adequate level of personal data protection. Consequently, in these cases, authorisation by ANSPDCP is not necessary.

#### b. **International transfer to states that do not offer an adequate level of personal data protection**

Such transfers can only be implemented upon prior authorisation by ANSPDCP, which is awarded only when appropriate guarantees for the protection of individuals' fundamental rights are stipulated in contracts compliant with the standard contractual clauses set forth by the European Commission Decision No. 2001/497/EC ("Data Transfer Contracts").

Data Transfer Contracts are not required when:

- data subjects have expressly consented to the transfer;
- the transfer is necessary for the execution of a contract between the data subject and the controller or between the controller and third parties, but for the benefit of the data subject;
- the transfer is necessary for a major public interest or the protection of the life, the physical integrity and health condition of the data subjects; or
- the transfer pertains to public data.

Data Transfer Contracts are also not required in the case of intra-group international data transfers when the group has implemented an internal code of conduct for international data transfers between group entities ("Binding Corporate Rules") that were previously approved by ANSPDCP. In such cases, notification of the transfer and authorisation by ANSPDCP are still required; however, the proceedings are more simplified and authorisation of the transfer is likely to be granted in a shorter term than in the case of transfers implemented based on Data Transfer Contracts.

### 11.2 Please describe the mechanisms companies 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, transfers to countries granting an adequate level of protection do not raise major issues for the controller.

As for transfers to countries not granting an adequate level of protection, the companies commonly transfer the personal data either based on a Standard Data Transfer Agreement, or upon consent of the data subjects.

In relation to both mechanisms, ANSPDCP generally assesses the equivalence between the information in the Standard Data Transfer Contract/consent notice and the information in the notification.

Recently, more and more companies are implementing Binding Corporate Rules for international transfers of data between group entities in order to hasten proceedings for authorisation of the transfer.

### 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 to countries outside the EU/EEA and not granting an adequate level of protection can be made only upon notification to ANSPDCP. Transfer to countries not granting an adequate level of protection, based on a Standard Data Transfer Contract and Binding Corporate Rules, requires authorisation by ANSPDCP.

## 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.)?

ANSPDCP has not issued any binding regulations on the implementation of corporate whistle-blower hotlines; however, the guidelines in Opinion No. 1/2006 of the European Commission's Data Protection Working Party ("Opinion No. 1") should be observed.

Implementation of whistle-blowing schemes is possible only if necessary:

- *for compliance with a legal obligation of the controller* – implementation of whistle-blowing schemes is mandatory by law in specific fields. Government Emergency Ordinance No. 99/2006 on credit institutions and capital adequacy sets forth the obligation of credit institutions to implement appropriate schemes for reporting breaches of banking regulations, providing, however, for an adequate standard of personal data protection, both for the whistle-blower and for the incriminated person, in accordance with the rules under the Personal Data Law; or
- *to pursue a legitimate interest of the controller or of a third party to whom data are disclosed* – corporate concern to prevent fraud and internal misconduct might be deemed as a legitimate interest justifying the implementation of whistle-blowing schemes. Nevertheless, implementations of such schemes can be done only if the relevant principles in the Personal Data Law are observed, in particular the proportionality, data minimisation and retention rules. Furthermore, reported employees should be informed about the purpose of the whistle-blowing scheme, the alleged accusations, the recipients of the data collected through the whistle-blowing scheme, and how to exercise their rights of access and ratification. However, in cases where there is a significant risk that the information of the incriminated person would jeopardise the effectiveness of the investigation, this may be delayed for as long as the risk exists.

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

The applicable legislation does not contain any specific rules. However, according to the recommendations in Opinion No. 1, anonymous reporting should be discouraged. Anonymous reporting may be permitted in exceptional cases and only under specific terms detailed in Opinion No. 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)?**

The processing of personal data by video surveillance may be performed for the following purposes:

- (i) criminal prevention and control;
- (ii) traffic surveillance;
- (iii) protection of individuals, assets, values, locations and equipment of public interest, as well as of the related areas;
- (iv) implementation of public interest measures or the exercise of public authority; and
- (v) safeguarding of legitimate interests, provided that the fundamental rights and freedoms or interests of the data subject are not prejudiced.

Prior notification to ANSPDCP is required.

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

Yes. CCTV data is allowed for the fulfilment of any legal obligations or based on a legal interest which basically is the safety of individuals, assets and areas.

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

The processing of personal data of employees by video surveillance means is allowed for the fulfilment of any legal obligations or based on a legal interest, with the observance of the employees' rights, especially regarding the prior notification of such.

If the above circumstances are not met, the processing of employees' personal data cannot be performed without the express and freely given prior consent of the employees.

The use of hidden video cameras or in locations which require the protection of individuals' intimacy is forbidden.

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

Please refer to question 14.1 above. The consent of employees is usually obtained in writing. The notification of the employees is also made in writing, usually by posting a relevant notice at the places where video cameras are located.

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

The processing of personal data by video surveillance means, for the legitimate purposes under question 14.1 above, does not require the notification or consultation of the employees' representatives or trade union.

**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 security of personal data is an obligation for both the controllers and processors. Order 52/2002 sets forth the minimum security standards for the processing of personal data, which aim mainly at: the implementation of appropriate measures for the identification and login of authorised users; access by each user only to the data necessary for their professional attributions; collection of personal data only by authorised persons and on authorised terminals; execution of security copies; implementation of access logs and encryption systems; secure deletion of unnecessary or outdated data; as well as the training of staff on the rules regarding lawful personal data 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) expects voluntary breach reporting.**

There is no statutory obligation of controllers to report data breaches to ANSPDCP except for the providers of publicly available electronic communication services who must promptly notify ANSPDCP about data breaches.

The notification shall include at least a description of the data breach and the contact details where more information can be obtained, as well as recommended measures to mitigate the possible negative effects of the breach. The notification will include a description of the consequences of the data breach and of the actions already implemented or proposed by the provider to address 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) expects voluntary breach reporting.**

There are no statutory rules compelling the operator to report data breaches to individuals.

However, in the electronic communications field, when the breach could affect the personal data or privacy of a subscriber or any other individual, the supplier must immediately notify the concerned subscriber or individual about such a breach. Notification is not required if the provider can attest that it has applied to the data affected by the security breach appropriate and effective security measures. The same obligation of information subsists in the case of a potential risk of data. If the risk exceeds the scope of the measures that providers can take, they must inform the subscribers about possible remedies and the relevant costs.

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

Failure to comply with the obligations regarding implementation of appropriate personal data security measures and personal

data confidentiality is incriminated as a contravention under the Personal Data Law and is sanctioned with a fine amounting between approximately EUR 330 and approximately EUR 11,100 (in national currency equivalent).

Furthermore, under Law No. 506/2004, failure to comply with the obligations regarding confidentiality and securing of the personal data processed in the field of electronic communications is sanctioned with a fine amounting between approximately EUR 1,100 and approximately EUR 22,200 (in national currency equivalent). For companies with an annual turnover exceeding the national currency equivalent of approximately EUR 1,100,000, such fines may reach 2% of the turnover.

## 16 Enforcement and Sanctions

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

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
Preliminary investigations: Upon notification and before processing, in connection with processing operations which may trigger special risks to the individuals' fundamental rights and freedoms.	ANSPDCP has the right to apply administrative fines ranging between approximately EUR 1,100 and approximately EUR 11,000 (in national currency equivalent), and to order temporary suspension or complete cessation of unlawful processing activities.	Whenever there is a reasonable assumption that a criminal offence might have been committed by means of unlawful personal data processing, ANSPDCP shall notify the competent criminal investigation authorities.
Ordinary investigations upon complaint or <i>ex officio</i> : ANSPDCP may request from the controller any information related to the processing (including professional and state secrecy) and may verify any relevant document or registration.	N/A	N/A

### 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. ANSPDCP has the right to issue a ban in relation to a particular processing without the need of a court order.

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

The main approach of ANSPDCP is to require the businesses to remedy the findings discovered during the investigations and to apply administrative sanctions if the breaches proved to be significant and merely recurrent. We have no information as to whether the ANSPDCP has issued a ban in relation to a specific processing.

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

No, as far as we know.

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

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

In Romania, e-discovery requests are dealt with in different ways depending on the nature of the request.

In civil matters, the legal framework is set forth by Law No. 175/2003 on Romania's accession to the 1970 Hague Convention on the taking of evidence abroad in civil or commercial matters (the "Hague Convention"). Under the Hague Convention, a judicial authority of a signatory state can request Romanian authorities to take evidence, intended only for use in ongoing or contemplated judicial proceedings. Moreover, diplomatic officers or consular agents of a signatory state can take evidence from Romania in aid of judicial proceedings commenced in the state which they represent. Nonetheless, in order for the pre-trial discovery procedure to be lawful, the processing of personal data needs to be legitimate and to satisfy one of the grounds set forth in the Personal Data Law.

In criminal matters, e-discovery by national companies in connection with trans-national criminal investigations can only be requested by national authorities who are entitled to take evidence based on letters rogatory. Consequently, companies cannot disclose personal data directly to foreign law enforcement agencies.

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

In relation to this topic, ANSPDCP has not issued any guidance.

## 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, ANSPDCP paid particular attention to the ways the controllers have obtained the data subjects' consent for the processing of personal data for different purposes, both in the online environment as well as offline.

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

Following the enactment of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27<sup>th</sup> 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 GDPR"), ANSPDCP has initiated several campaigns for increasing awareness among the controllers with respect to the new requirements of the GDPR. In this respect, the authority has organised seminars, workshops and roundtables having as attendees and speakers stakeholders from the private, as well as the public, sector. Moreover, ANSPDCP has launched a guideline with relevant information regarding the implementation of the GDPR.

## Acknowledgment

The authors would like to thank Cosmina Sima, Junior Associate at Pachiu & Associates, for her invaluable assistance in the preparation of the chapter. Email: [cosmina.sima@pachiu.com](mailto:cosmina.sima@pachiu.com).

**Mihaela Cracea**

Pachiu & Associates  
13 Barbu Delavrancea Street  
Bucharest 1  
RO-011351  
Romania

Tel: +40 21 312 1008  
Fax: +40 21 312 1009  
Email: [mihaela.cracea@pachiu.com](mailto:mihaela.cracea@pachiu.com)  
URL: [www.pachiu.com](http://www.pachiu.com)

Mihaela is a lawyer with over 14 years of professional experience. She coordinates the IT and data privacy department of the firm as well as the labour and employment sub-practice groups.

Mihaela has built solid expertise and legal competence in the IT, data protection and intellectual property fields and manages data privacy projects in the digital field, information security and cross-border data flow matters.

Other highlights of Mihaela's practice involve holding seminars on the measures to be implemented, so as to ensure data privacy and cybersecurity compliance. She also reviews IT and data privacy policies and other related documentation in terms of local and European statutory provisions in the field.

As a labour and employment lawyer, she has been involved in projects on staff restructuring and transfer of undertakings by providing guidelines, drafting the required documentation, assisting the clients during the negotiations and following up on the post-acquisition issues.

She is a graduate of the Faculty of Law of the Ovidius University in Constanta and holds an LL.M. degree in Business Law and is an intellectual property counsel on trademarks. She is fluent in English and conversant in French and co-authored several *International Comparative Legal Guides* focusing on data protection matters and digital environment and attended, as a speaker, several local conferences on cybersecurity and data privacy.

**Alexandru Lefter**

Pachiu & Associates  
13 Barbu Delavrancea Street  
Bucharest 1  
RO-011351  
Romania

Tel: +40 21 312 1008  
Fax: +40 21 312 1009  
Email: [alexandru.lefter@pachiu.com](mailto:alexandru.lefter@pachiu.com)  
URL: [www.pachiu.com](http://www.pachiu.com)

A lawyer with over 12 years of professional experience, Alexandru is a Partner coordinating the firm's **Corporate and M&A Department**.

As head of the Corporate Practice Group (including the Labour Law, Competition, Insolvency and IP sub-practice areas), his practice covers corporate governance and restructuring (mergers, spin-offs, capital restructuring, etc.), intricate joint venture deals and takeover/divestment procedures, as well as private equity funds in complex transactions, including greenfield and brownfield developments. Alexandru has also been involved in financing and insurance matters and constantly advises on competition, insolvency, labour law and recently on several IT deals.

Alexandru plays a key role in the core management team, being in charge of the smooth delivery of all projects in the Corporate Practice Group, supervising and coordinating client and internal practice development.

Alexandru is a graduate of the Faculty of Law of the University of Bucharest and holds an LL.M. awarded by Suffolk University Law School in Boston. He also holds a degree from the Institute of Business Law and International Cooperation "Henri Capitant" – a partnership of the Faculties of Law of the University of Bucharest and Pantheon-Sorbonne, Paris.



ATTORNEYS AT LAW · RECHTSANWÄLTE · ABOGADOS

Our firm's **IT & Data Protection Practice Group** is focused on data privacy, intellectual property and e-commerce related matters featuring a dedicated team of lawyers enthusiastic when faced with the intricate challenges of the digital field, and a dynamic industry undergoing continuous development.

The main legal services we provide:

- Verifying legal compliance of projects aimed at the acquisition of companies active in the online environment.
- Drafting and/or reviewing documents required for notifying the data protection authority in terms of personal data processing.
- Verifying compliance of policies, regulations and agreements used by clients in their online businesses.
- Analysing compliance of personal data transfers to third countries which fail to provide a level of protection similar to the one at European level.
- Verifying compliance of policies, regulations and agreements used by clients in their online businesses.
- Analysing risks in the relationships between companies and employees with a view to secure intellectual property rights in favour of companies.
- Verifying policies, regulations and internal practices to secure compliance with the legal requirements on the processing of the personal data of employees, participants to various promotional campaigns, and webpage users for all intents and purposes.
- Any other data protection and intellectual property related matters encountered by clients in their businesses.

For further reference about us, please visit [www.pachiu.com](http://www.pachiu.com).



# 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 Senegalese Data Protection Authority (*Commission de Protection des Données Personnelles*) (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 and economic identity.

#### ■ “Processing”

“Processing” of personal data (or “Data Processing”) means any operation or set of operations in relation to such data, especially its 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, or jointly or in common with other persons) takes the decision to collect and process personal data and determines the purposes of the processing.

#### ■ “Processor”

“Processor” means all persons who (either alone, or jointly or in common with other persons) collect, exploit, register, organise, store, adapt, modify, retrieve, backup, copy, consult, use or disclose data by transmission, dissemination or otherwise making available, alignment, locking, encryption, erasure or destruction.

#### ■ “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 to such data, especially its interception, misappropriation, damage, deletion, erasure, alteration, counterfeiting by an unauthorised production, use, backup or transfer process.

#### ■ Other key definitions – please specify (e.g., “Pseudonymous Data”, “Direct Personal Data”, “Indirect Personal Data”)

There are no other specific key definitions.

### 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.
- *Other key principles – please specify*  
**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 its personal data forms part of the processing.
  - A copy of its 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 information relating to the 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 rectifies or deletes their personal data if it is 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**  
Relating to the right to deletion, 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**  
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:
  - If required by the law.
  - To fulfil a general interest mission or required by the public authority.
  - For an agreement execution 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.
- *Other key rights – please specify*  
There are no other specific key rights.

## 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 its processing activities, except in the following cases:

- Non-profit processing for religious, philosophical or political associations, or trade unions (when the data corresponds with the purpose of the association or trade union, and concerns only their members and is 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 protection authority without any consideration on the fact that 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 by the 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 involves an interconnection of files.
- Data that includes a national identification number.
- Biometric data.
- Data that is 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 as long as it is 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 but 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 Senegalese Data Protection Authority website – <http://www.cdp.sn/repertoire-des-declarations>.

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

A typical notification process takes one month, unless extended by a motivated decision from the CDP, once.

## 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 to 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 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 to object to all messages sent to him.

### 9.2 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.

### 9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

Yes, the restrictions above apply to marketing sent from other jurisdictions.

### 9.4 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 the data protection law.
- HELLO FOOD SENEGAL was sent a warning on 15 May 2015 for failure to respect the data protection law.
- DIGITAL VIRGO was sent a warning on 31 July 2015 for failure to respect the legal prospecting terms.
- EXPRESSO TELECOM was summoned on 20 October 2017 for failure to respect the data protection law.
- CBAO ATTIJARIWAFI BANK was summoned on 20 October 2017 for failure to respect the data protection law.

#### 9.5 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.

#### 9.6 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 and a XOF 1 million fine, or only one of these sentences.

## 10 Cookies

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

There is no provision relating 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?

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?

This is not applicable in Senegal.

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

This is not applicable in Senegal.

## 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 companies 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 to privacy, liberty and fundamental rights to Data Subjects. Before transferring personal data, the company must inform the CDP. The information must précis:

- 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 concerned persons.
- 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, the exercise or defence of a legal right in court; and
- perform an agreement between the Data Subject and the Data Processor or precontractual measures taken on 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 reasoned request, if the Data Processor offers sufficient guarantees to 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 was supposed 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 of 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.

## 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 and binding guidance issued by the CDP on corporate whistle-blower hotlines.

### 12.2 Is anonymous reporting prohibited, or strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do companies 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 requires prior authorisation of 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 self-security purposes when used by individuals. If so, the CCTV system must only cover the house perimeter.
- For security and infringement prevention or recognition in public areas, the reasons why it is used by public authorities.
- For business premises security and access or employees' movement control 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 the 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.
- 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 the data 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 introduced in the system is 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 to preserve it.

**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) expects 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) expects 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 criminal maximum penalty for security breaches is imprisonment for one (1) to seven (7) years and a fine of between XOF 500,000 and XOF 10 million, or one of these penalties. 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).**

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
<p>The CDP can conduct three types of investigation:</p> <ul style="list-style-type: none"> <li>■ On-site inspections</li> </ul> <p>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.</p> <ul style="list-style-type: none"> <li>■ Documentary inspections</li> </ul> <p>These inspections allow the CDP to obtain disclosure of documents or files upon written request.</p> <ul style="list-style-type: none"> <li>■ Hearing inspections</li> </ul> <p>These inspections consist of interrogation in their offices or summoning representatives of Data Controllers in order to obtain any necessary information.</p>	<p>The CDP can impose the following sanctions in cases of breach of the DPA:</p> <ul style="list-style-type: none"> <li>■ provisional withdrawal for three months of the given authorisation; the withdrawal becomes definitive at the end of the three-month period if the breach remains; and</li> <li>■ fines of between XOF 1 million and XOF 100 million.</li> </ul> <p>In cases of urgency, the CDP can also:</p> <ul style="list-style-type: none"> <li>■ interrupt the processing for a duration which cannot exceed three months;</li> <li>■ lock certain kinds of data for a duration which cannot exceed three months; and</li> <li>■ prohibit provisionally or definitively processing which does not comply with the DPA.</li> </ul>	<p>Criminal sanctions are pronounced by Courts. They are:</p> <ul style="list-style-type: none"> <li>■ imprisonment for a period of between six months and seven years; and</li> <li>■ fines of between XOF 200,000 and XOF 10 million.</li> </ul>

**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 a 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 their processing. 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 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 companies established in other jurisdictions? If so, how is this enforced?**

The CDP does not exercise its powers against companies established in other jurisdictions.

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

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

We have no information on how companies 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 CDP current “hot topic” 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, up until now, no legal measure has been taken to this end.



#### Léon Patrice Sarr

LPS L@w  
Cité Keur Gorgui Immeuble Elysée II  
5ème étage, appartement 18  
Dakar  
Senegal

Tel: +221 33 848 79 88

+221 30 106 57 57

Email: [lp.sarr@lps-law.com](mailto:lp.sarr@lps-law.com)

URL: [www.lps-law.com](http://www.lps-law.com)

Mr. Sarr is the Managing 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.

His practice areas include:

- Information and Technology.
- Intellectual Property.
- Mergers and Acquisitions.
- Energy and Natural Resources.



LPS L@w is known to offer services which are above customers' expectations. It reflects our passion for the work, the cutting-edge training of our team and our experience in international organisations. We are therefore adequately prepared to satisfy both international standards and local market needs.



# Singapore

OrionW LLC

Winnie Chang



## 1 Relevant Legislation and Competent Authorities

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

The principal data protection legislation in Singapore is the Personal Data Protection Act 2012 (No. 26 of 2012) (**PDPA**). The PDPA governs the collection, processing and protection of personal data by private organisations and establishes the ‘Do Not Call Registers’ (**DNC Registers**).

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

The Computer Misuse Act (**CMA**) prohibits unauthorised access to any program or data held in any computer and the unauthorised modification of the contents of any computer.

The new Cybersecurity Act imposes duties on owners of critical information infrastructure to comply with cybersecurity codes of practice and standards, implement cybersecurity incident-reporting measures and conduct regular audits and risk assessments.

The Spam Control Act (**SCA**) regulates the bulk sending of unsolicited commercial electronic messages to an email address or mobile telephone number. The SCA requirements are discussed in question 9.1 below.

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

Several sector-specific laws and regulations set out data protection obligations, including:

- the Banking Act, which prohibits banks in Singapore from sharing customer information with third persons, except where expressly permitted thereunder;
- the Code of Practice for Competition in the Provision of Telecommunications Services 2012 under the Telecommunications Act, which governs the use and disclosure of information that is obtained by telecommunications licensees from end-users; and
- the Infectious Diseases Act and the Private Hospitals and Medical Clinics Act, which contain provisions relating to the confidentiality of medical information.

In the event of any inconsistency between the PDPA and another written law, the latter’s provisions will prevail to the extent of the inconsistency.

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

The PDPA is administered and enforced by the Personal Data Protection Commission (**PDPC**) in Singapore. Sector-specific data protection obligations are enforced by the relevant sectoral regulators, with the PDPC’s co-operation.

## 2 Definitions

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

#### ■ “Personal data”

The PDPA defines “personal data” 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 has or is likely to have access’.

#### ■ “Processing”

The PDPA defines “processing”, in relation to personal data, as the ‘carrying out of any operation or set of operations in relation to the personal data, and includes any of the following: recording; holding; organisation, adaption or alteration; retrieval; combination; transmission; erasure; or destruction’.

#### ■ “Controller”

The PDPA does not use the term “controller”, but generally refers to a person that determines the purposes for and the manner of processing personal data as an “organisation”. The PDPA defines “organisation” as including ‘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”

The PDPA uses the equivalent concept of “data intermediary” instead of the term “processor”. A “data intermediary” is ‘an organisation which processes personal data on behalf of another organisation but does not include an employee of that other organisation’.

#### ■ “Data Subject”

The PDPA uses the term “individual” *in lieu* of “data subject” to refer to an individual who is the subject of personal data. The PDPA defines “individual” as ‘a natural person, whether living or deceased’.

#### ■ “Sensitive Personal Data”

The PDPA does not impose additional obligations on

organisations for processing personal data which are deemed 'sensitive'. Therefore, the term "sensitive personal data" is not used in the PDPA. However, a data breach involving sensitive personal data can be considered an aggravating factor which could lead to the PDPC meting out a higher financial penalty (see question 16.3 below).

- **"Data Breach"**  
"Data breach" is not defined in the PDPA. However, the PDPC has referred to "data breach" as 'the unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks of personal data in an organisation's possession or under its control'.
- *Other key definitions – please specify (e.g., "Pseudonymous Data", "Direct Personal Data", "Indirect Personal Data")*  
This is not applicable.

### 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 private organisations that collect or process personal data in Singapore, including organisations that are not physically in Singapore (see the definition of "organisation" in question 2.1 above). For example, the PDPA applies to foreign companies that collect personal data in Singapore via websites.

### 4 Key Principles

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

- **Transparency**  
An organisation must inform an individual of its purposes for collecting, using or disclosing his personal data (unless an exception applies) and make available to the public the business contact information of at least one of its Data Protection Officers (see section 7 below for more information on Data Protection Officers) ("**Notification Obligation**").  
An organisation must also develop and implement data protection policies and practices to comply with the PDPA and make them publicly available ("**Openness Obligation**").
- **Lawful basis for processing**  
The PDPA is anchored on the fundamental principle of consent whereby an individual's consent (express or deemed) must be obtained before his personal data are collected, used or disclosed for any purpose, unless an exception under the PDPA or any other written law applies ("**Consent Obligation**").
- **Purpose limitation**  
Under the PDPA, an individual's personal data may only be collected, used or disclosed for purposes that a reasonable person would consider appropriate in the circumstances and of which the individual concerned has been informed, if notification is required ("**Purpose Limitation Obligation**").
- **Data minimisation**  
The principle of data minimisation is reflected in the Purpose Limitation Obligation. An organisation also cannot, as a condition of providing a product or service, require an individual to consent to the processing of his personal data beyond what is reasonable to provide that product or service.

Organisations must limit their retention of collected data under the Retention Limitation Obligation (as defined below).

- **Proportionality**  
An organisation should determine what a reasonable person would consider appropriate in the circumstances when fulfilling the Data Protection Obligations (as defined below). Under the PDPC's non-binding advisory guidelines, a "reasonable person" is 'a person who exercises appropriate care and judgment in the particular circumstances'.
- **Retention**  
An organisation must destroy or dispose of personal data in its possession or control, or anonymise personal data, when personal data are no longer required for the purpose for which they were collected or no longer serve any legal or business purposes ("**Retention Limitation Obligation**").
- *Other key principles – please specify*
  - **Accuracy**  
An organisation must exert reasonable effort to ensure the accuracy and completeness of personal data collected by it or on its behalf if such data are likely to be disclosed or be used to make a decision affecting the individual concerned ("**Accuracy Obligation**").
  - **Protection**  
An organisation must implement reasonable security arrangements to protect personal data in its possession or control against unauthorised access, collection, use, disclosure, copying, modification, loss, disposal or similar risks ("**Protection Obligation**").
  - **Transfer Limitation**  
The PDPA prohibits the transfer of personal data outside Singapore except where the transferred data are provided a standard of protection that is comparable to the protection under the PDPA ("**Transfer Limitation Obligation**"). See also question 11.1 below.  
(The Consent Obligation, Purpose Limitation Obligation, Notification Obligation, Access Obligation (see question 5.1 below), Correction Obligation (see question 5.1 below), Accuracy Obligation, Protection Obligation, Retention Limitation Obligation, Transfer Limitation Obligation and Openness Obligation are collectively referred to as the "**Data Protection Obligations**".)

### 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 access (a) their personal data which an organisation possesses or controls, and (b) information on the use or disclosure of such personal data within a year before the access request ("**Access Obligation**").  
An individual may also request for a physical or electronic copy of his personal data. If a copy cannot be produced, the individual may be given a reasonable opportunity to examine the requested data in person.  
There are exceptions to the Access Obligation. For example, an organisation may refuse an access request where the requested data relates to opinion data kept solely for an evaluative purpose or where the request is frivolous or vexatious.  
Moreover, an organisation is prohibited from granting an access request in certain instances, such as where doing so can reasonably be expected to threaten the safety or physical/mental

health of another individual or where the organisation lawfully disclosed personal data to a prescribed law enforcement agency without the requesting individual's consent.

■ **Right to rectification of errors**

Individuals have a right to the correction of any error or omission in their personal data ("**Correction Obligation**"). An organisation which corrects personal data must send the corrected data to each organisation that received the original data within a year before the correction date, unless that other organisation no longer needs the corrected data.

There are exceptions to the Correction Obligation. For example, an organisation may refuse to correct an opinion.

■ **Right to deletion/right to be forgotten**

This is not applicable.

■ **Right to object to processing**

See 'Right to withdraw consent' below.

■ **Right to restrict processing**

See 'Right to withdraw consent' below.

■ **Right to data portability**

This is not applicable.

■ **Right to withdraw consent**

An individual may, by reasonable notice to an organisation, withdraw his consent for the collection, use and/or disclosure of his personal data for any purpose.

■ **Right to object to marketing**

An individual may (a) by notice to an organisation, withdraw his consent to use his Singapore telephone number for messages sent by SMS, phone or fax, or (b) opt out of receiving unsolicited telemarketing messages by adding his Singapore telephone number to the DNC Registers.

■ **Right to complain to the relevant data protection authority(ies)**

An individual may file a complaint with the PDPC regarding an organisation's PDPA violation.

■ *Other key rights – please specify*

- An aggrieved individual who suffered loss due to a Data Protection Obligation violation has a right to file a civil action for relief (e.g., damages or an injunction) against an erring organisation.

## 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 organisations to register with or notify the PDPC or any other governmental body in respect of its 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)?**

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.

An organisation must appoint at least one Data Protection Officer (DPO) and must make the DPO's business contact information publicly available.

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

The PDPC may direct an erring organisation to appoint a DPO. See also question 16.1 below on other sanctions that may be imposed.

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

The PDPA does not expressly protect the DPO from disciplinary measures, or other employment consequences, in respect to the individual's role as a DPO. However, under the PDPA, an organisation, not its DPO, remains legally responsible for complying with the PDPA.

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

The PDPA does not prohibit the appointment of a single DPO to cover multiple entities.

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

The PDPA does not specify any qualifications for the DPO. However, a DPO should have appropriate expertise and knowledge to ensure that he or she can fulfil this role.

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

A DPO is responsible for (a) ensuring the appointing organisation's compliance with the PDPA, (b) developing and implementing the organisation's data protection policies and processes, (c) handling data protection queries and complaints relating to the organisation, (d) highlighting any data protection risks to the organisation, and (e) liaising with the PDPC on the organisation's behalf.

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

There is no registration/notification requirement for the appointment of a DPO. However, organisations are encouraged to register their DPOs with the PDPC.

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

The PDPA does not prescribe the types of information that an organisation must include in a public-facing privacy notice or equivalent document to fulfil its Notification Obligation (see question 4.1 above). However, an organisation must make its DPO's business contact information publicly available (see question 7.1 above) and the PDPC recommends that such information be included in its 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?

It is not mandatory for an organisation to execute a written agreement with its data intermediary. However, a data intermediary that processes personal data on an organisation's behalf under a contract evidenced or made in writing will be exempt from the Data Protection Obligations, except the Protection Obligation and the Retention Limitation Obligation.

### 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 an organisation remains responsible for complying with the PDPA in respect of personal data processed by its data intermediary, it is prudent for an organisation to impose obligations on its data intermediary through a written agreement which restricts what the data intermediary can do with the disclosed personal data and requires the data intermediary to (a) act only according to the organisation's instructions, (b) have sufficient security measures to secure and protect such data, and (c) comply with the PDPA.

## 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 Do Not Call (DNC) provisions of the PDPA, organisations must obtain an individual's consent before collecting, using or disclosing his personal data for marketing purposes, unless an exception applies.

However, if an organisation will send a marketing message to an individual's Singapore telephone number by SMS, phone or fax (**specified message**), it may only send such message if it (a) obtains consent, which is clear, unambiguous and in writing or any other accessible form, to send the specified message, (b) checks the relevant DNC Register(s) within the prescribed period before sending, or (c) has an ongoing relationship with the individual and has complied with certain conditions, including that the specified message will be sent by SMS or fax only.



A specified message must include clear and accurate information identifying the organisation and its contact details. Telephone numbers used to make telemarketing calls should not be concealed.

Under the SCA, the following information should be included when sending bulk unsolicited commercial emails or text messages (**spam messages**):

- a clear and conspicuous statement in English that an unsubscribe request can be submitted;
- a title in the subject field, if any, and header information that is not false or misleading;
- the letters <ADV> with a space before the title in the subject field or, if there is no subject field, the first word of the message; and
- an accurate and functional email address or telephone number by which the sender is readily contactable.

The unsubscribe facility must be valid and capable of receiving a reasonable number of unsubscribe requests at all times for a period of at least 30 days after spam messages are sent. Spam messages should no longer be sent after 10 business days following the submission of an unsubscribe request.

The SCA applies concurrently with the PDPA. Thus, organisations must comply with the SCA and check the No Text Message DNC Register before sending unsolicited text marketing messages in bulk.

The PDPC is considering consolidating the DNC provisions in the PDPA and the SCA into a single legislation governing all unsolicited commercial messages. Under the new legislation, the DNC provisions will apply to unsolicited marketing messages sent to Singapore telephone numbers, whilst the SCA provisions will be extended to apply to unsolicited commercial text messages that are sent in bulk to instant messaging identifiers (i.e., account ID or login ID) created by users on instant messaging platforms such as Facebook or WeChat.

---

**9.2 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 question 9.1 above.

---

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

---

The restrictions in question 9.1 above apply to marketing sent from other jurisdictions if the recipient of the marketing message is present in Singapore when the marketing message is accessed.

---

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

---

The PDPC has been active in enforcing marketing restriction offences since the PDPA marketing restrictions came into force in January 2014.

---

**9.5 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 containing personal data constitutes a “collection” of personal data under the PDPA. It is unlawful to purchase such marketing lists from third parties, unless the

individuals are notified of and consent to the sale of their personal data before such data are collected, used and/or disclosed.

---

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

---

The maximum financial penalty for sending marketing communications that violate the Data Protection Obligations is S\$1 million. However, breaching the marketing restrictions relating to specified messages discussed in question 9.1 above could be a criminal offence which is subject to a fine of up to S\$10,000 per offence.

---

## 10 Cookies

---



---

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

---

The PDPA does not expressly regulate cookies (or similar technologies); the Data Protection Obligations apply to cookies which are personal data.

---

**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?**

---

To date, the PDPC has not issued any enforcement decisions in relation to cookies.

---

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

---

See question 9.6 above for the maximum penalties for breaches of the Data Protection Obligations. The PDPA does not impose cookie-specific restrictions.

---

## 11 Restrictions on International Data Transfers

---



---

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

---

See the discussion on the Transfer Limitation Obligation in question 4.1 above.

The recipient of transferred personal data should be bound by legally enforceable obligations (e.g., law, contract or binding corporate rules (where the recipient is related to the transferring organisation)) which require it to protect the transferred data in a manner that is at least comparable to the protection under the PDPA. This requirement is deemed satisfied in certain instances, such as where an individual consents to the transfer of personal data to a recipient in a specified jurisdiction or the transfer of personal data is necessary for the performance of a contract between the individual and the transferring organisation.

**11.2 Please describe the mechanisms companies 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 typically incorporate terms in their contracts whereby individuals consent to the transfer of personal data abroad. Companies also use data transfer agreements and binding corporate rules to transfer personal data abroad to comply with the Transfer Limitation Obligation.

**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.**

Transfers of personal data to other jurisdictions do not require registration/notification or prior approval from the PDPC.

## 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 regulate corporate whistle-blower hotlines.

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

The PDPA does not regulate anonymous reporting.

## 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)?**

Separate registration/notification or PDPC approval is not required for CCTV use. However, an organisation must comply with the Consent Obligation and Notification Obligation when using CCTVs, unless an exception applies. That said, as best practice, notice of CCTV use for any purpose should be provided even when it is not required, e.g., by placing notices of CCTV use in prominent locations.

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

The use of CCTV data which constitute personal data is subject to the Purpose Limitation Obligation.

## 14 Employee Monitoring

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

The PDPA permits employee monitoring for the purpose of managing an employment relationship (e.g., monitoring how an employee uses company computer network resources). However, employers should ensure that employee monitoring does not breach the CMA. For instance, unauthorised access to data by logging into an employee's personal email account without the employee's consent is an offence under the CMA.

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

Employers are required to inform employees of the purposes for which such monitoring is carried out, but consent is not required. Employers may provide notice to and obtain consent from their employees through express terms in their employment agreements, policies or manuals.

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

There are no statutory requirements to notify or consult work councils/trade unions/employee representatives in this regard. The extent of notification or consultation will ultimately depend on the terms of the collective agreement between an employer and the trade union.

## 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.)?**

See the discussion on the Protection Obligation in question 4.1 above. The Protection Obligation applies to all organisations and data intermediaries that collect and process 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) expects voluntary breach reporting.**

As of February 2018, there is no legal requirement to report data breaches to the PDPC. As best practice, the PDPC advises organisations to notify the PDPC, as soon as possible, of any data breach that might cause public concern or where there is a risk of harm to a group of affected individuals.

The PDPC has been considering imposing a mandatory notification requirement where a data breach is likely to result in significant harm or impact to affected individuals or where the scale of the breach is significant. If this requirement is imposed, organisations will have to notify the PDPC within 72 hours, and affected individuals as soon as practicable, after the time the organisation determines that the breach is eligible for reporting.

**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) expects voluntary breach reporting.**

As of February 2018, the PDPA does not require organisations to report data breaches to affected individuals. However, organisations may be contractually obligated to notify individuals affected by a data breach. Organisations may also soon be required to notify affected individuals of a data breach (see question 15.2 above).

As best practice, the PDPC advises organisations to notify affected individuals, immediately if the breach involves sensitive personal data or, in other cases, when the breach is resolved.

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

See question 9.6 above for the maximum penalties for breaches of the Data Protection Obligations.

## 16 Enforcement and Sanctions

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

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
On a complainant's application, to review (a) a refusal of an access or correction request or failure to provide access or to make a correction within a reasonable time, or (b) a fee for processing an access request	The PDPC may: (a) require the approval of an access or correction request; or (b) reduce or disallow a fee for processing an access request, or require a refund to the complainant.	Fine of up to S\$5,000 (for individuals) or S\$50,000 (for entities) that dispose of, alter, falsify, conceal, destroy personal data to evade an access or correction request.
To give directions to any organisation that contravenes the Data Protection Obligations	This includes directions to: (a) stop processing personal data in contravention of the PDPA; (b) destroy personal data collected in contravention of the PDPA; and (c) comply with a PDPC direction relating to an access or correction request; and (d) pay a financial penalty of up to S\$1 million.	Not applicable

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
To require documents or information and to enter premises with or without warrant	Not applicable	Fine of up to S\$10,000 and/or imprisonment of up to 12 months for individuals, or fine of up to S\$100,000 for entities for obstructing the PDPC in its functions/powers or providing false/misleading 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 PDPC has the power 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 such direction.

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

The PDPC seeks to balance individuals' need to protect their personal data and organisations' need to use those data for legitimate purposes. The PDPC generally encourages self-resolution by a complainant and an erring organisation; however, the PDPC will likely pursue an investigation where the breach indicates a systemic failure to comply with the PDPA, affects a large group of people or causes loss, injury or other damage, or where the public interest requires.

The PDPC will consider the seriousness of a breach and the effectiveness of an organisation's remedial measures in imposing a financial penalty.

Recent cases include:

- **Breach of Protection Obligation**  
A financial penalty of S\$30,000 was imposed on an insurance company for failing to make reasonable security arrangements to prevent the unauthorised disclosure of personal data of policyholders. The substantial financial penalty was in part due to the fact that this was the insurance company's second case within a period of 12 months.
- **Unauthorised Sale of Personal Data**  
A financial penalty of S\$6,000 was imposed on an individual for the unauthorised sale of a database containing personal data. In imposing the financial penalty, the PDPC considered the sensitivity of the personal data sold and the individual's actions in obscuring her identity when selling the database.
- **Breach of Protection and Retention Obligations**  
A financial penalty of S\$18,000 was imposed on an organisation for failing to protect the personal data of its clients' customers and failing to remove their personal data from its website. Several aggravating factors were considered in imposing the financial penalty, including the organisation's delayed remedial action, misleading the PDPC and its generally uncooperative attitude during the investigation process.

- **Breach of Protection Obligation**

A financial penalty of S\$15,000 was issued to an organisation for failing to implement reasonable security arrangements to protect its members' personal data. The substantial financial penalty was due to the number of potentially affected individuals and the failure to identify and rectify security vulnerabilities earlier.

- **Breach by a Data Intermediary**

A financial penalty of S\$10,000 was imposed on a data intermediary for failing to have reasonable security arrangements to protect the personal data of its client's customers. The sensitivity of the personal data disclosed and the unauthorised modification of millions of individuals' personal data were factors that the PDPC considered in imposing the financial penalty.

---

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

---

The PDPC has yet to exercise its powers against companies established in other jurisdictions. However, the PDPC may establish arrangements with foreign data protection regulators, which may include cross-border cooperation, to enforce the PDPA against erring foreign companies.

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

---

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

---

Companies typically provide in their privacy policies or customer contracts for disclosure of personal data to local and foreign law enforcement agencies if required to do so.

---

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

---

To date, the PDPC has not issued any guidance pertaining to e-discovery or 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.**

---

Out of the 23 enforcement decisions issued by the PDPC in the 12 months from April 2017, 16 of the enforcement decisions concerned the Protection Obligation (see question 16.3 above for a summary of several enforcement decisions).

---

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

---

As of February 2018, the PDPC has been considering additional grounds for collecting, using and disclosing personal data to include, subject to certain conditions, instances where an individual is notified of the purposes for processing his personal data and does not opt out of such processing or where an organisation has legitimate interests to process personal data without consent. The PDPC is also reviewing the need for mandatory data breach notifications to the PDPC and affected individuals (see question 15.2 above).

In addition, the PDPC published two new non-binding guides on data sharing and data anonymisation in early 2018.



**Winnie Chang**

OrionW LLC  
Level 42  
6 Battery Road  
Singapore 049909

Tel: +65 6232 2361  
Email: [winnie.chang@orionw.com](mailto:winnie.chang@orionw.com)  
URL: [www.orionw.com](http://www.orionw.com)

Winnie Chang is the Managing Director at OrionW and leads its Technology, Media and Telecommunications (**TMT**) practice. She has advised on a wide range of cutting-edge TMT and FinTech transactional and regulatory projects, data protection, cybersecurity, corporate and commercial, encryption, and export regulatory compliance projects for local and international clients.

Winnie has over 17 years of experience in TMT practice areas in Singapore and the United Kingdom. She received the 2014 Finance Monthly Global Award for 'TMT Lawyer of the Year' in Singapore, and was recognised by *The Legal 500 Asia Pacific* 2017 edition as having "long experience in TMT, excellent industry knowledge and attention to detail".

Winnie is the author of *A Practical Guide to Singapore Data Protection Law*, a concise and practical guide on data protection issues in Singapore. She is a contributor to the 'Communications' volume of *Halsbury's Laws of Singapore* and co-author of the chapter on *Cryptography and Electronic Signatures* in a publication launched at the UN World Summit on the Information Society.



OrionW is a boutique law firm specialising in Singapore and cross-border commercial, corporate and regulatory matters, with a focus on technology, media and telecommunications (**TMT**) and financial technology (**FinTech**) law. Its lawyers and consultants have decades of experience in major international law firms and companies in Asia, Europe and the US. The firm is known for its exceptional legal expertise, deep industry knowledge, commercial pragmatism and a commitment to providing high-quality solutions for clients.

Based in Singapore, OrionW is privileged to work with Fortune 50, FTSE 100 and multinational companies in the TMT, FinTech, financial services, life sciences, logistics, aviation and retail sectors. OrionW also advises innovative start-ups and SMEs as they expand their business operations throughout Asia. The firm advises on sophisticated commercial and corporate transactional projects, and TMT, FinTech, data protection, cybersecurity, anti-corruption and export control regulatory projects in Asia. OrionW has won various awards and its work has been recognised by *The Legal 500*, *Asialaw Profiles*, *APAC Insider* and *Corporate INTL*.

# Spain

Carlos Pérez Sanz



Pia Lestrade Dahms



Ecija Abogados

## 1 Relevant Legislation and Competent Authorities

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

Currently, the principal data protection legislation is the Spanish Data Protection Act 15/1999 (the “**LOPD**”). Royal Decree 1720/2007 (the “**RLOPD**”) is ancillary to the LOPD and sets out security measures for personal data and further regulation. However, this regulation is set to be modified.

From 25 May 2018, the principal data protection legislation in the EU will be Regulation (EU) 2016/679 (the “**General Data Protection Regulation**” or “**GDPR**”). The GDPR repeals Directive 95/46/EC (the “**Data Protection Directive**”) and leads to increased (though not total) harmonisation of data protection law across the EU Member States. In Spain, a draft bill (the “**Draft LOPD Bill**”) is currently before the Spanish Parliament (please note: these answers were written before the Draft LOPD Bill was adopted; consequently, they might not reflect the final adopted text). This bill is intended to repeal the current LOPD and any provisions of equal or inferior category that contradict, oppose or are incompatible with the GDPR and the Draft LOPD Bill. Further, in its current version, the Draft LOPD Bill is intended to enter into force from 25 May 2018.

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

Organic Law 1/1982 on civil protection of the rights to honour, personal and family privacy and an individual’s own image.

Gross privacy non-disclosure violations might be prosecuted under criminal charges in accordance to Art. 197 of the Criminal Code.

Law 34/2002 on information society services and ecommerce (the “**LSSI**”). This law covers the e-marketing communications regime, internet service provider (ISP) liability and anti-spam regulation.

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

A large number of sector-specific legislation is available. A few examples are listed below:

- (a) Art. 96 of the Spanish Consumer Rights Act *Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias*, in connection with Art. 29 of *Ley 3/1991 de 10 de enero, de competencia desleal*, as modified by Law 29/2009.

- According to this regulation, marketing phone calls must be clearly identified as such, and fully disclose the identity of the calling company. In every communication, recipients shall be offered the opportunity to oppose to further calling. Human operators are allowed for telemarketing only. Recorded telemarketing campaigns need the prior recipient to opt-in.
- (b) Art. 41 of the Spanish Telecoms Act *Ley 9/2014, de mayo, General de Telecomunicaciones* sets forth privacy standards for telecommunications, including compulsory notifications to the Data Protection Authority (the “**DPA**”) and to data subjects in the case of breaches or violations of security. Art. 48 further provides that customers’ geolocation information (latitude data) should always be processed anonymously. Nominal customer geolocation is only allowed when strictly necessary and indispensable for the provision of value-added services expressly requested by the customer. In such a case, the customer should be informed about the extent, purpose and duration of this processing.
- (c) Insurance legislation such as *Real Decreto Legislativo 6/2004, de 29 de octubre, por el que se aprueba el texto refundido de la Ley de ordenación y supervisión de los seguros privados* and *Ley 26/2006, de 17 de julio, de mediación de seguros y reaseguros privados* contains data protection provisions specific to the insurance industry.
- (d) Legislation specific to healthcare service provisions sheds light on rights to access health records and mandatory conservation timeframes of such information. The most important piece of legislation is *Ley 41/2002, de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica*.
- (e) Art. 17 of *Ley 59/2003 de firma electrónica* covers data privacy issues related to electronic signatures.
- (f) *Real Decreto 1553/2005, de 23 diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica* covers electronic identity card usage.
- (g) Art. 6.2b of *Ley 11/2007 de Acceso electrónico de los ciudadanos a los servicios públicos* provided the citizens’ right to get in touch with the public administration by electronic means. It has now been derogated by *Ley 39/2015, de 1 octubre, del Procedimiento administrativo común de las administraciones públicas*. The public administration must ensure security measures when handling a citizen’s data with regards to such communication.
- (h) The Spanish Data Retention Act *Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones*. This act governs carrier companies’ obligations to retain traffic and personal data related to such traffic.

- (i) Art. 20.3 of *Real Decreto Legislativo 2/2015, de 23 de octubre, del Estatuto de los Trabajadores*. This article sets out that control measures on employees are permitted.

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

The main data protection authority is the *Agencia Española de Protección de Datos* (the “**AEPD**” or “**Spanish DPA**”). However, there are also regional data protection authorities in Catalonia and the Basque Country with powers essentially over public entities within their respective territory.

## 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.
- *Other key definitions – please specify (e.g., “Pseudonymous Data”, “Direct Personal Data”, “Indirect Personal Data”).*  
There are no other key definitions to be aware of.

## 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 data subjects who are in the EU in relation to: (i) the offering of goods or services (whether or not in return for payment) to data subjects who are in the EU; or (ii) the monitoring of the behaviour of data subjects who are in the EU (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 data subjects who are in the EU (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 interest 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 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 competent data protection authority in Spain, if the data subjects live in Spain or the alleged infringement occurred in Spain.

#### ■ 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?

Under the LOPD/RLOPD, businesses must register with/notify the Spanish DPA before creating files containing personal data. They must also notify any modifications or cancellations of such files to the Spanish DPA (see the LOPD/RLOPD).



**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)?**

It must be specific. The specific forms are available on the Spanish DPA's website and cannot be submitted unless the required information is filled out.

**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 per legal entity and 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)?**

All of the above must register with the relevant data protection authorities.

**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 fields are the following:

- Information of the declarant.
- Information of the data controller (name, industry, CIF/NIF number and address).
- Valid address for exercising rights of access, opposition, rectification and erasure (if different).
- Information on relevant data processors (if any).
- File name.
- Purpose of processing.
- Source/origin of data.
- Categories of data under processing.
- Security level (basic, medium or high).
- Processing methods (automated, manual or mixed).
- Transfer of data to third parties (data surrender or disclosure).
- International transfers (for transfers outside of the European Economic Area).

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

Failing to notify files, or doing so in an inaccurate way, constitutes a minor infringement on the grounds of Art. 44.2.c of the LOPD (and will incur a fine of EUR 900 to EUR 40,000). Failure to notify files after being expressly mandated to do so by the DPA constitutes a serious infringement punishable by a fine of between EUR 40,001 and EUR 300,000.

**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)?**

There is no set renewal obligation for registrations/notifications. However, any modifications to the categories listed under question 6.5 must be notified. Further, a notification must also be submitted when a data processing stops taking place (is discontinued) or when data processing is transferred to a new data controller.

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

There is no prior approval required for these registrations/notifications. However, please note that prior approval may be required for international transfers.

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

Yes. They can be completed at the following address: <https://sedeagpd.gob.es/sede-electronica-web/>. However, please note that the procedure might not be able to be carried out entirely online.

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

Yes. However, not all information is made available to the public. For example, registration codes and security levels are not available publicly.

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

One (1) month.

## 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 Draft LOPD Bill provides an extensive list of when the appointment of a Data Protection Officer is mandatory:

- Professional associations which are regulated by Law 2/1974.
- Educational institutions which are regulated by Law 2/2006.

- Entities which exploit networks and provides electronic communications services when they process large-scale regular and systematic personal data.
- Society information service providers when they create large-scale profiles of users of the service.
- Entities covered by Law 10/2014 (credit entities).
- Financial establishments which are regulated by Law 5/2015.
- Insurance entities which are regulated by Law 20/2015.
- Investment services companies which are regulated by Royal Decree 4/2015.
- Electric energy distributors and suppliers as well as natural gas distributors and suppliers.
- Entities who are in charge of general files for assessing financial solvency and creditworthiness or general files for managing and preventing fraud, including controllers which are regulated by Law 10/2010.
- Entities engaged in advertising activities and commercial research, including commercial and market research, when they carry out processing activities based on preferences of data subjects or when they carry out processing activities which involve profiling of the data subjects.
- Health centres which are legally required to keep medical records of patients in accordance with Law 41/2002.
- Entities whose purposes include the issuance of commercial reports which could mention natural persons.
- Gaming operators whose activity is carried out electronically, telematically and interactively in accordance with Law 3/2011.
- Those who carry out activities which are regulated by Law 5/2014 (private security).

## 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.

Failure to comply with the requirement to designate a Data Protection Officer (when mandatory to do so) is considered a serious infringement under the Draft LOPD Bill.

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

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

The Draft LOPD Bill specifies that the appointed Data Protection Officer cannot be dismissed or penalised for performing his tasks, except in cases of intent or gross negligence.

## 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 (“DPIAs”) 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. More specifically, the Draft LOPD Bill indicates that controllers and processors shall notify designations and dismissals of Data Protection Officers within ten (10) days. This applies when the designation of a Data Protection Officer is mandatory as well as when the entity chooses to appoint one voluntarily.

## 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”) recommends 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 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 Data Protection Officer; (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.

The Spanish DPA has published Guidelines for the Preparation of Contracts between controllers and processors available at: [http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/EN\\_directricescontratos.pdf](http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/EN_directricescontratos.pdf) (English version).

## 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 Email, SMS and Other Electronic Means**

General opt-in rule: Unsolicited emailing requires previous opting in from the data subject.

Exceptional opt-out rule: Customers can be sent unsolicited emails, provided such unsolicited emailing is advertising similar goods and services to those previously purchased by such customers.

Single click unsubscribe: Such an option at the end of every post is mandatory.

The Robinson List: Must be checked before sending electronic communications.

**9.2 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.).**

**Regular Post**

Unsolicited marketing communications can only be sent in written paper format by regular post to individuals whose contact details are displayed in telephone directories or are obtained from other public sources.

**Phone Call**

The Spanish Consumer Rights Act *Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias* bans “robot” telemarketing phone

calls. Unsolicited telemarketing calls must be performed by human agents, and shall always show the phone number of the calling party. People in the Robinson List should never be contacted.

Art. 29 of the Spanish Unfair Competition Act *Ley 3/1991, de 10 de enero, de Competencia Desleal* considers it an aggressive practice to carry out persistent unsolicited phone calls, emails or any other electronic means, unless this is deemed necessary and justifiable in order to seek fulfilment of legal obligations.

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

Yes, they do.

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

Yes, they are.

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

Due regard shall be paid to the legal basis of the processing and the duty of information (Art. 13 of the GDPR and Art. 14 of the GDPR). Further, the purchaser must be able to demonstrate that it complies with the GDPR and, specifically, that the use of a purchased marketing list complies with any of the legitimate basis of processing as established by Art. 6 of the GDPR. The general rules on sending marketing communications apply.

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

Sending marketing communications in breach of the LSSI shall be fined up to EUR 150,000. However, if doing so involved an infringement of the LOPD at the same time, then an additional fine of up to EUR 300,000 shall be imposed.

## 10 Cookies

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

The LSSI implements Art. 5 of the EU ePrivacy Directive. Pursuant to Art. 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 Directive 95/46/EC and, from 25 May 2018, the GDPR). For consent to be valid, it must be informed, specific, freely given and must constitute a real 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, which means that it must be essential to fulfil their request. The Spanish DPA has published a Guide on Cookies available in Spanish.

**10.2 The EU Commission intends to pass a new ePrivacy Regulation that will replace the respective national legislation in the EU Member States. The regulation is planned to come into force May 25, 2018 and will provide amended requirements for the usage of cookies. Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?**

See the previous answer.

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

Yes. It is noteworthy to mention that a fine was imposed in 2017 for using the Mailchimp Service in breach of Art. 22.2 of the LSSI.

For other sanction resolutions, please visit the Spanish DPA's website: <http://www.agpd.es/portalwebAGPD/canaldocumentacion/cookies/index-ides-idphp.php>.

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

Failure to provide proper cookie information might attract fines of up to EUR 30,000. If this action is repeated within three (3) years after the first final decision of the Spanish DPA, this might attract fines from EUR 30,000 to EUR 150,000.

## 11 Restrictions on International Data Transfers

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

Data transfers to 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) or the business has implemented one of the required safeguards as specified by the GDPR.

**11.2 Please describe the mechanisms companies 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.

Transfer of personal data to the US is also possible if the data importer has signed up to the EU-US Privacy Shield Framework, which was designed by the US Department of Commerce and the EU Commission to provide businesses in the EU and the US with a mechanism to comply with data protection requirements when transferring personal data from the EU to the US.

**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.

## 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. The WP29 recommends 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, or 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, the WP29 considers 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.

Traditionally, Spain prohibited anonymous reporting (see the Spanish DPA's legal report 2007-0128). However, the Draft LOPD Bill opens the door to anonymous reporting.

## 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)?

According to the LOPD, prior notification is needed as for any other type of personal data processing. Further, controllers must place a sign which is sufficiently visible, and documents which comply with the duty to inform must be made available to data subjects.

Under the GDPR, a 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 Draft LOPD Bill follows essentially what has been outlined under the current LOPD.

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

A guide on video surveillance is set to be published by the Spanish DPA once the GDPR and the new LOPD become applicable.

## 14 Employee Monitoring

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

Monitoring must be lawful, transparent, proportionate and legitimate and there should not be other less intrusive means to reach equivalent goals. Prominent video surveillance signs are always a must.

In 2017, the WP29 updated its opinion on data processing at work (Opinion 2/2017).

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

Consent of employees is not needed, since notice is required since control measures on employees are permitted by law (Art. 20.3 of *Estatuto de los trabajadores*), provided that such control measures comply with the above-mentioned principles. The Draft LOPD Bill adds that failure to provide the required information will not deprive the images of their probative value where the images have captured the flagrant commission of a criminal act. However, this is without prejudice to the liabilities that may arise from such failure.

The issue of notice in the context of covert video surveillance of employees has been the subject of a recent case of the ECHR (*López Ribalda v. Spain*).

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

The Company's Workers' Committee (*comités de empresa*) must be informed of the existence of CCTV, according to Art. 64.2 of *Estatuto de los trabajadores*.

## 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 EUR 20 million or 4% of worldwide turnover.

Further, failure to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk as is required by Art. 32.1 of the GDPR is considered a serious infringement under the Draft LOPD Bill.

## 16 Enforcement and Sanctions

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

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
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.	N/A
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).	N/A
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.	N/A
Imposition of Administrative Fines for Infringements of Specified GDPR Provisions	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.	N/A

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
Non-Compliance With a Data Protection Authority	The GDPR provides for administrative fines which will be EUR 20 million or up to 4% of the business' worldwide annual turnover of the proceeding financial year, whichever is higher.	N/A

**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 Spanish DPA makes all its decisions available to the public. Therefore, there are countless enforcement examples available on the Spanish DPA's website.

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

Yes. Just recently the Spanish DPA imposed fines on Facebook, Inc. and Whatsapp, Inc. (see Resolution R/00259/2018). The preliminary questions revolved around the applicable law. The Spanish DPA concluded that:

- Facebook Spain, S.L. was an establishment of Facebook Inc.: Spanish Law is applicable when the data are processed in the context of activities conducted at the controller's establishment, provided such establishment is located on Spanish soil (see Art. 2.1.a) of the current LOPD).
- Facebook, Inc. processed data with hardware located on Spanish soil which was not employed for transit only: Spanish Law is applicable when the controller is not established in the European Union and processes the data with hardware located on Spanish soil, unless such hardware is employed for transit only (see Art. 2.1.c) of the current LOPD).
- Whatsapp, Inc. did not have an establishment in Spain nor in any other country of the EEA when it published its update of the Terms of Service and Privacy Policy. Nevertheless, it was using hardware located on Spanish soil which was not employed for transit only (see Art. 2.1.c) of the current LOPD).

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

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

Businesses will typically analyse the request on a case-by-case basis and take into account data protection, labour, criminal and other relevant laws. They will check, among others, if the request is correctly made, if it complies with the legal formalities between the countries, the scope of the request, the legal basis for the disclosure and any international data transfer issues.

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

No clear guidance is in place besides international conventions ratified by Spanish regulatory bodies, such as the USA FTC Memorandum of Understanding and equivalent documents. However, the WP29's Working Document 1/2009 on pre-trial discovery for cross-border civil litigation might provide some guidance. Further, the Spanish DPA analysed the issue in 2011 and published a legal report which is available on its website.

## 18 Trends and Developments

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

Sanction procedure resolutions of the Spanish DPA have dealt mostly with the following:

- Art. 4.3 of the LOPD – Quality of data.
- Art. 6.1 of the LOPD – Data subject consent.
- Art. 21 of the LOPD – Prohibition of commercial communications sent by electronic means without previous data subject consent.

Also noteworthy is that the Spanish DPA has imposed fines on Facebook, Whatsapp and Google in the last twelve (12) months.

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

The GDPR and the Draft LOPD Bill are the two main "hot topics".

**Carlos Pérez Sanz**

Ecija Abogados  
Av. Diagonal, 458  
8<sup>th</sup> floor  
08006 Barcelona  
Spain

Tel: +34 933 808 255  
Email: [cperez@ecija.com](mailto:cperez@ecija.com)  
URL: [www.ecija.com](http://www.ecija.com)

**Partner and Head of Information Technology at ECIIA**

With a professional background of more than 20 years in advising leading Spanish and International companies on matters related to information technology, telecommunications, intellectual property, privacy law and compliance regulations, Carlos Pérez Sanz developed most of his career in Landwell – PwC Tax & Legal Services, which he joined in 1998. In PwC, he has been a partner and the Head of the Information Technology Department of the firm in Spain. Carlos Pérez Sanz holds an LL.B. from Universidad de Barcelona, an M.B.A. from ESADE in Barcelona, and is an associated professor at the same university for its Intellectual Property and Information Society Master's programme. In addition, he holds the International CISA Certification as a qualified information technology systems' auditor by ISACA (Information Systems Audit and Control Association).

Carlos Pérez Sanz has played an active role during his professional career in the elaboration process of numerous regulations related to new technology law; in particular, related to the Spanish Data Protection Act, Intellectual Property Act and Information Society Act.

He has been selected as one of the best lawyers in information technology and data protection law in Spain by the prestigious international rankings *The Legal 500* and *Best Lawyers International*.

**Pia Lestrade Dahms**

Ecija Abogados  
Av. Diagonal, 458  
8<sup>th</sup> floor  
08006 Barcelona  
Spain

Tel: +34 933 808 255  
Email: [plestrade@ecijalegal.com](mailto:plestrade@ecijalegal.com)  
URL: [www.ecija.com](http://www.ecija.com)

**Information Technology at ECIIA**

Pia Lestrade Dahms is a member of the Florida Bar in the United States. She holds a B.A. in Political Science from the University of Connecticut, a J.D. from St Thomas University, and a Master's in Intellectual Property and Information Society from ESADE. She has volunteered at technology-related conferences organised by the French Member of Parliament who represented French citizens living in North America. Further, she also volunteered at the first edition of the Startup Europe Awards by providing analysis on the French startup landscape. She is a member of the International Association of Privacy Professionals and speaks English, French, Spanish and Catalan.

# ECIIA

ECIIA is among the Top 10 best law firms in the Spanish market (*Chambers Europe* and *The Legal 500 2017*) which received the 2017 Expansión Awards for most innovative law firm, and best information technology, intellectual property, and data protection law firm. It also received that same year the Forbes Awards for law firm of the year for the aforementioned fields from Forbes.

Established in 1997 with a focus on TMT and IP, the firm has grown since then to become a full-service firm with presence in all areas of law and in every sector. ECIIA comprises a team of first-class lawyers with outstanding experience and is broadly international in scope. It is lauded for service, quality and client satisfaction.

While ECIIA is a full-service firm and provides a range of legal services, we offer distinctive specialisation in some areas linked to the most developed sectors of industry: ECIIA is the Spanish reference in technology, media, and telecommunications law.

The firm has offices in Madrid, Barcelona, Valencia, Lisboa, Miami, and Santiago de Chile, and collaborates in many other worldwide jurisdictions as the sole Spanish member of MERITAS, the largest worldwide lawyers' network, with more than 7,000 lawyers in over 70 countries around the world.

For further information, please visit [www.ecija.com](http://www.ecija.com).

# Sweden

Mattias Lindberg



Marcus Lorentzon



## Affärsadvokaterna i Sverige AB

### 1 Relevant Legislation and Competent Authorities

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

The EU Regulation (EU) 2016/679 (the “**General Data Protection Regulation**” or “**GDPR**”) will enter into force 25 May 2018. When in force, the GDPR will be the principal data protection legislation in the EU. Under the GDPR, the data protection legislation across the EU Member States will be more harmonised, though not in total since there are a lot of other data protection acts that still will be in force (e.g. covering areas such as healthcare and financial activities).

As a result of the GDPR, Sweden will get a new Data Protection Act (“**DPA**”). The new DPA will complement the GDPR in regard to the areas in which the GDPR opens up for national legislation.

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

The Camera Surveillance Act and the Electronic Communications Act implement the ePrivacy Directive 2002/58/EC. The European Convention on Human Rights has been incorporated into Swedish law which, primarily for the purpose of data protection, has an impact on the Swedish principle of openness (Sw. *offentlighetsprincipen*) and freedom of the press and freedom of speech (Sw. *tryck- och yttrandefriheten*).

The EU Commission has also proposed a new regulation on privacy and electronic communications that will apply to telecom and internet operators and replace the current Directive 2009/136/EC. The ePrivacy Regulation would harmonise the applicable rules across the EU.

The DPA authorises the government and the Swedish data protection authority, the Data Inspection Board (“**DIB**”), to issue more detailed regulations concerning several features of the DPA.

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

Hundreds of acts and ordinances contain regulations for registration and Processing of Personal Data, covering areas such as healthcare and financial activities.

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

According to the GDPR, it is mandatory for each EU Member State

to provide for one or more supervisory authority/authorities to be responsible for monitoring the application of the GDPR. In Sweden, the Swedish data protection authority, the DIB, is responsible for the monitoring of the data protection legislation.

The DIB ensures that authorities, companies, organisations and individuals follow (i) the GDPR (as of 25 May 2018), (ii) the *old* Data Protection Act (until 24 May 2018), (iii) the Data Act, (iv) the Debt Recovery Act, and (v) the Credit Information Act.

The DIB works to prevent intrusion upon privacy through information and by issuing directives and codes of statutes. The DIB also handles complaints from individuals and organisations and carries out inspections. Inspections may be triggered by complaints but are normally planned and conducted in campaigns for sector-specific areas.

### 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.
- “**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 Subject**” means an individual who is the subject of the relevant Personal Data.
- “**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 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.
- **“Pseudonymisation”** means 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.
- **“Consent”** of the Data Subject means any freely given, specific, informed and unambiguous indication of the Data Subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to him or her.

### 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, since the GDPR harmonises the data protection legislation across the EU Member States, some of the data protection laws apply to businesses outside of Sweden. All businesses that process Personal Data, either as a Controller or Processor, and that are established in any EU Member State, fall under the scope of the GDPR, regardless of whether or not the Processing takes place in the EU.

Furthermore, the GDPR applies to businesses that are established outside the EU, either if they are subject to the laws of an EU Member State or if they are Processing Personal Data of EU residents to be able offer goods or services or to monitor the behaviour of EU residents (if 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 in relation to the Data Subject. This means that the Controller must provide the Data Subject with certain minimum information, provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language, regarding the collection and Processing of the Personal Data.
- **Lawful basis for processing**  
It is only lawful to process Personal Data to the extent it is permitted under EU data protection law. According to the GDPR, Processing of Personal Data is permitted if: (i) the Data Subject has given Consent to the Processing of his or her Personal Data for one or more specific purposes; (ii) Processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract; (iii) Processing is necessary for compliance with a legal obligation to which the Controller is subject; (iv) Processing is necessary in order to protect the vital interests of the Data Subject or of another

natural person; (v) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller; or (vi) Processing is necessary for the purposes of the 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 which require protection of Personal Data, in particular where the Data Subject is a child.

Processing of sensitive Personal Data, such as data concerning health, political opinion or religious beliefs, require stronger legal grounds than regular Personal Data.

- **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. In certain cases, a Controller may use the relevant Personal Data in a manner that is incompatible with the purposes for which they were initially collected.

- **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.

- **Accuracy**

Personal Data must be accurate and, where necessary, kept up to date, hence the Controller 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 Personal Data being processed; (iv) information about the categories of recipients with whom the Personal Data may be shared; (v) information about the period for which the Personal Data will be stored (or the criteria used to be determine that period); (vi) information about the existence of the rights to erasure, to rectification, to restrict 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 Personal 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.

#### ■ **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 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 Personal 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 Personal 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 Personal Data may only be held by the Controller, and may only be used for limited purposes if: (i) the accuracy of the Personal 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 Personal 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 right not to be subject to a decision based solely on automated processing**

The Data Subject has the right not to be subject to a decision based solely on automated Processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

#### ■ **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 DIB, if the Data Subjects lives in Sweden or the alleged infringement occurred in Sweden.

#### ■ **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?**

The Data Protection Directive 95/46/EC and the old DPA prescribed for a general obligation to notify Processing of Personal Data to the DIB. This obligation led to administrative and financial burden but did not always improve personal protection. Therefore, the GDPR does not contain any such obligations. Instead of the general obligation to notify the supervisory authority, the GDPR prescribes that the Controller shall perform a data protection impact assessment ("DPIA") or a prior consultation with the supervisory authority if the Processing is likely to, or would, result in a high risk to the rights and freedoms of natural persons.

### 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 DPIA and a prior consultation with the supervisory authority may concern a single data Processing operation. However, a single assessment may address a set of similar Processing operations that present similar high risks.

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

DPIAs and prior consultations shall be made per data processing operation. Several Controllers may perform joint DPIAs and prior consultations.

### 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)?**

If a Controller is established in more than one EU Member State or is carrying out cross-border Processing, the Controller may establish a lead supervisory authority that will handle all cases related to the Processing. Otherwise, the supervisory authority of the main or single establishment of the Controller is competent to be the supervisory 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)?**

A DPIA shall contain at least: (i) a systematic description of the envisaged Processing operations and the purposes of the Processing, including, where applicable, the legitimate interest pursued by the Controller; (ii) an assessment of the necessity and proportionality of the Processing operations in relation to the purposes; (iii) an assessment of the risks to the rights and freedoms of Data Subjects; and (iv) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data and to demonstrate compliance with the GDPR, taking into account the rights and legitimate interests of Data Subjects and other persons concerned.

A prior consultation with the supervisory authority shall contain: (i) where applicable, the respective responsibilities of the Controller, joint Controllers and Processors involved in the Processing, in particular for Processing within a group of undertakings; (ii) the purposes and means of the intended Processing; (iii) the measures and safeguards provided to protect the rights and freedoms of Data Subjects pursuant to the GDPR; (iv) where applicable, the contact details of the Data Protection Officer; (v) a DPIA; and (vi) any other information requested by the supervisory authority.

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

Non-compliance with a DPIA and prior consultation requirements can lead to fines of up to €10 million or 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

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

This is not applicable in Sweden.

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

This is not applicable in Sweden.

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

There is no such requirement in Sweden.

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

This is not applicable in Sweden.

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

There is no such list.

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

The supervisory authority shall, within a period of up to eight weeks from receipt of the request for consultation, provide written advice to the Controller.

**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.**

In some circumstances it is mandatory for Controllers and the Processors to appoint a Data Protection Officer. The most relevant circumstances being large-scale and systematic monitoring of individuals and/or large-scale Processing of sensitive Personal Data.

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

If the Controller or Processor fail to comply with a mandatory appointment of a Data Protection Officer, the Controller or Processor may be penalised with any penalties available under the GDPR.

**7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect to 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?**

Yes, 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.

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

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 Personal 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 DPIAs 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)?

The Controller or Processor must notify the DIB of the contact details of the Data Protection Officer.

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

No. 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, a Controller that appoints a Processor 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. To be able to fulfil the requirements of the GDPR, it is essential for the Controller to appoint a Processor that 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 Data Protection Officer; (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 the 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?)

The Marketing Act has regulations on marketing by email, fax or telephone. Under the Marketing Act, a trader may, in the course of marketing to a natural person, use email, a telefax or automatic calling device or any other similar automatic system for individual communication that is not operated by an individual, only if the natural person has Consented to this in advance. Where a trader has obtained details of a natural person's email address in the context

of a sale of a product to that person, the Consent requirement shall not apply, provided that (i) the natural person has not objected to the use of the email address for the purpose of marketing via email, (ii) the marketing relates to the trader's own similar products, and (iii) the natural person is clearly and explicitly given the opportunity to object, simply and without charge, to the use of such details for marketing purposes, when they are collected and in conjunction with each subsequent marketing communication.

In marketing via email, the communication shall, at all times, contain a valid address to which the recipient can send a request that the marketing cease. This also applies to marketing to a legal person. A trader may use methods for individual marketing communication other than those referred to above, unless the natural person has clearly objected to the use of such methods.

According to the GDPR, the Data Subject shall have the right to object at any time to Processing of Personal Data concerning him or her for direct marketing purposes, which includes profiling to the extent that it is related to such direct marketing. Where the Data Subject objects to Processing for direct marketing purposes, the Personal Data shall no longer be processed for such purposes.

### 9.2 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 Marketing Act prescribes that traders may use means of distance communication other than, for example, SMS and email, for marketing purposes unless the natural person clearly opposes the use of the method.

Good marketing practice requires marketers – before a call is made to a consumer in sales, marketing or fundraising purposes – to control if the consumer's phone number is in the blocking registry (NIX-Telefoni). The blocking registry is an opt-out registry which includes, from the year 2015, both regular phones and mobile phones. If a control is made, the company is entitled to call the consumer within two months from the day on which the used version of the track log was updated.

### 9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

The Marketing Act applies to foreign companies provided that they target the marketing to a Swedish audience.

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

Yes, it is.

### 9.5 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. Marketers need to follow good marketing practice, which includes sector-specific ethical rules.

### 9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

Breaches of the restrictions in the Marketing Act may result in a



penalty. In recent years, a standard of 5,000,000 Swedish kronor has been used. In addition, both traders and natural persons may claim damages.

Furthermore, traders may be ordered to pay a special charge (market disruption charge) if the trader, or a person acting on behalf of the trader, intentionally or negligently contravenes obligations in the Marketing Act. The market disruption charge shall be fixed at no less than 5,000 Swedish kronor and no more than 5,000,000 Swedish kronor. However, the charge may not exceed 10% of the trader's annual turnover.

## 10 Cookies

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

The Electronic Communications Act states that information may be stored in or retrieved from a subscriber's or user's terminal equipment only if subscribers or users are provided with access to information on the purpose of the Processing and Consents to the Processing. For Consent to be valid, it must be informed, specific, freely given and must constitute a real indication of the individual's wishes.

This does not apply to the storage or retrieval necessary for the transmission of an electronic message over an electronic communications network, or for the provision of a service explicitly requested by the subscriber or user.

### 10.2 The EU Commission intends to pass a new ePrivacy Regulation that will replace the respective national legislation in the EU Member States. The regulation is planned to come into force May 25, 2018 and will provide amended requirements for the usage of cookies. Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

The proposed rules will ensure that users get better control over their privacy settings and can easily Consent or deny cookies. According to the proposal, you do not need to Consent to the use of harmless cookies that make the site more user-friendly. For example, cookies that enable the service provider to remember what is in the customers "shopping cart" or to keep track of the number of visitors on a website will not require Consent.

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

Yes, the Swedish Post and Telecom Authority (Sw. "PTS") has carried out supervision in respect of the Processing of data and obtaining Consent in relation to cookies. The supervisions include how the companies obtain their respective Consent to use cookies. The PTS has thereafter produced a preliminary assessment based upon those supervisions on obtaining Consent in its endeavour for the general public to have greater insights and more influence over how personal information is used in connection with the use of telephones and the internet. A final assessment from the PTS will only be available in the respective decisions in regards to the supervisions of the respective companies. No such final assessments have been rendered yet. Hence, the preliminary standpoints are not binding but may nevertheless be indicative for companies who must observe the regulations on Consent in the Electronic Communications Act.

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

The penalty for breaches is a fine. The amount varies depending on the circumstances.

## 11 Restrictions on International Data Transfers

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

In principle, data transfers to jurisdictions outside of the European Economic Area (the "EEA") are not permitted. Data transfers to a jurisdiction outside the EEA can only take place if the Data Subject Consents to the transfer, if transfer is to an "Adequate Jurisdiction" or if the business has implemented one of the required safeguards as specified by the GDPR.

### 11.2 Please describe the mechanisms companies 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.

For smaller businesses, the easiest way to comply with the data transfer rules is to get the Consent of the Data Subject or to carry out the data transfer as a result of the performance of a contract with the Data Subject.

For international businesses, data transfer to a jurisdiction outside of the EEA can be safeguarded by the implementation of Binding Corporate Rules ("BCRs"). The BCRs will always need approval from the relevant data protection authority.

Furthermore, businesses can adopt the Standard Contractual Clauses drafted by the EU Commission. The Standard Contractual Clauses are available for transfers between Controllers, and transfers between a Controller and a Processor.

Transfer of Personal Data to the US is also possible under the EU-US Privacy Shield Framework.

### 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.

Yes, most of the safeguards outlined in the GDPR will need initial approval from the DIB.

## 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 hotlines are generally established in order to

implement proper corporate governance principles in the daily functioning of businesses. However, the company must comply with the fundamental requirements of the GDPR, and therefore have a legal ground; for example, for the Processing and provision of sufficient information to the Data Subjects.

The WP29 recommends 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, or strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?**

As there is no specific statute or guidance, anonymous reporting is not strictly prohibited or strongly discouraged under EU data protection law.

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 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.

## **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 Camera Surveillance Act regulates the use of equipment for audio-visual monitoring and surveillance. In general, permission is required for camera surveillance of sites to which the public has access, but sometimes a notification is sufficient.

From the data privacy perspective, 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 prior to any action being taken by the Controller, the Controller must consult the DIB.

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

CCTV monitoring may be used to prevent, investigate and reveal crimes, prevent accidents and other comparable purposes.

## **14 Employee Monitoring**

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

Employee monitoring is subject to the general requirements of the DPA/GDPR. However, in the opinion of the DIB, employers cannot rely on Consent from employees to the Processing of Personal

Data that occurs when an employee monitoring system is used. This is because employees often find themselves in a position of dependence upon their employers and are therefore unable to give the voluntary Consent required by the DPA/GDPR.

It has become more and more common for employers to use positioning systems of various kinds to check where their employees are.

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

Employers typically obtain Consent either by the employment agreement or by referencing the company's data protection policy. The employer can also justify its actions by a balance of interests in accordance with the DPA/GDPR.

It should be noted that in the opinion of the DIB, employers cannot rely on Consent from employees to the Processing of Personal Data. This is because employees often find themselves in a position of dependence upon their employers and are therefore unable to give the voluntary Consent demanded by the DPA/GDPR. Employers who want to use employee monitoring must normally rely on a balance of interests. The employer's interest in carrying out the Processing must then outweigh the employee's interest in protection from an invasion of privacy. In the overall assessment that must be performed in these cases, the following factors must be considered: (i) the purpose of the Processing; (ii) how the data are handled and how the results are used; (iii) what information is given to the employees; (iv) whether the Processing can be performed in a way that involves less invasion of privacy; (v) what technical and administrative security is available for the data; (vi) the existence of collective agreements and the content of these; and (vii) whether the Processing follows good practice for the labour market.

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

There is no absolute requirement to receive an approval from the relevant trade union. However, in the balance of interests in accordance with the DPA/GDPR, the opinion of the trade union may become an important factor. It is therefore important for the employer (and the Data Protection Officer) to have a good and productive relationship with the trade unions in the discussions of whether the Processing follows good practice for the labour market or not. Hence, it is normally well-invested time to initiate a discussion with the relevant trade union at an early stage in the process.

## **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 Processor must ensure they have appropriate technical and organisational measures to meet the requirements of the GDPR. Depending on the security risk, this may include (i) the encryption of Personal Data, (ii) the ability to ensure the ongoing confidentiality, integrity and resilience of Processing systems, (iii) an ability to restore access to data following a technical or physical incident, and (iv) 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.**

Yes, 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 DIB, 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, so that the Controller can report the Data Breach to the DIB.

The notification must include (i) the nature of the Personal Data Breach including the categories and number of Data Subjects concerned, (ii) contact details of the Data Protection Officer, (iii) the likely consequences of the breach, and (iv) 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 (i) the contact details of the Data Protection Officer, (ii) the likely consequences of the breach, and (iii) any measures taken to remedy or mitigate the breach.

Under some circumstances, the Controller may be exempt from notifying the Data Subject (e.g. if the risk of harm is remote or if the Controller has taken measures to minimise the risk).

**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 Power	Civil/Administrative Sanction	Criminal Sanction
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.	N/A
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).	N/A
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.	N/A
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 proceeding financial year.	N/A

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
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.	N/A

### 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.

Consistent enforcement of the data protection rules is central to a harmonised data protection regime. The WP29 has created a document that is intended to ensure consistent application and enforcement of the GDPR. The powers described under question 16.1 will enter into force on 25 May 2018. Initially, the supervisory authorities are likely to use caution when exercising these powers.

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

Each supervisory authority shall ensure that the imposition of administrative fines pursuant to the GDPR. In case of cross-border Processing of Personal Data, the Controller shall establish a lead supervisory authority. However, the Data Subject may file a complaint to the local supervisory authority. The GDPR requires lead and concerned supervisory authorities to co-operate, with due respect for each other's views, to ensure a matter is investigated and resolved to each authority's satisfaction – and with an effective remedy for Data Subjects.

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

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

The concept of e-discovery does not exist in Sweden. However, the parties in civil cases under some circumstances have a duty of disclosure. There is no duty to disclose information to foreign law enforcement agencies.

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

There is no such guidance.

## 18 Trends and Developments

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

In Sweden, there is an extreme focus on integrity in both the strategic agreements and in GDPR projects as such. This trend is partly because of the new EU regulations but due to a large scandal, regarding the government's use of Personal Data and data security, during the summer of 2017.

The Swedish market is placing more and more focus on privacy issues in general by internally improving its processes in regards to quality. The DIB is encouraging entities to build privacy and data protection measures into the design of their data Processing in order to facilitate compliance with privacy and data protection principles. Hence, there is a lot of work going on so that authorities, companies, organisations and individuals will be able to meet the challenges resulting from the GDPR and the use of new technologies.

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

In general, the DIB is increasingly placing emphasis on the advice towards companies and organisations to conduct integrity analysis when taking important business decisions with regards to privacy issues.

The legislator is working hard to implement the data protection reform and update other registry legislation to function with the GDPR.

**Mattias Lindberg**

Affärsadvokaterna i Sverige AB  
Västra Trädgårdsgatan 15  
111 53 Stockholm  
Sweden

Tel: +46 708 13 05 18  
Email: [mattias.lindberg@affarsadvokaternasverige.se](mailto:mattias.lindberg@affarsadvokaternasverige.se)  
URL: [www.affarsadvokaternasverige.se](http://www.affarsadvokaternasverige.se)

Mattias Lindberg is the founding partner of Affärsadvokaterna i Sverige AB.

Mattias Lindberg has broad experience in providing legal advice and suggested measures in local and multi-jurisdictional outsourcing, strategic agreements, IT law and privacy law.

As a Data Privacy expert, Mattias Lindberg has extensive experience of analysing and implementing business-critical processes for the handling of personal data. He takes a methodical and pedagogic approach when analysing, optimising and implementing authority-regulated operational processes. As the personal data protection officer for several companies, Mattias Lindberg has extensive experience of implementing operational processes in accordance with the General Data Protection Regulation and the Patient Data Act.

Mattias Lindberg provides advice concerning all aspects of personal data management and regularly produces strategies regarding how personal data should be implemented and handled, and how integrity analysis should be conducted. Mattias Lindberg places particular focus on ensuring that the information is not only handled in accordance with the applicable laws and regulations, but that it is also handled in as practical and cost-effective a manner as possible. In addition, Mattias Lindberg has a great deal of experience in handling both ongoing contacts with the Data Inspection Board and audits conducted by the Board. He is also a highly-regarded public speaker, and is regularly invited to speak on various aspects of commercial law.

**Marcus Lorentzon**

Affärsadvokaterna i Sverige AB  
Västra Trädgårdsgatan 15  
111 53 Stockholm  
Sweden

Tel: +46 705 09 77 22  
Email: [marcus.lorentzon@affarsadvokaternasverige.se](mailto:marcus.lorentzon@affarsadvokaternasverige.se)  
URL: [www.affarsadvokaternasverige.se](http://www.affarsadvokaternasverige.se)

Marcus Lorentzon is an associate at Affärsadvokaterna i Sverige AB.

Marcus Lorentzon has extensive experience within the fields of IT law and privacy law and provides advice concerning all aspects of privacy law. Marcus also holds experience of implementing operational processes in accordance with the General Data Protection Regulation and the Patient Data Act.

Furthermore, Marcus is specialised in tort and insurance law and has for several years worked within the insurance industry. Marcus is used to working with both the legal and commercial risks that companies face in their business and has good knowledge in managing and eliminating such risks.



AFFÄRSADVOKATERNA

Affärsadvokaterna is a modern firm focused on commercial law. Affärsadvokaterna offers legal services of the highest quality and with the greatest commitment. Affärsadvokaterna offers advice mainly in regards to strategic agreements, privacy law, IT law, outsourcing, dispute resolutions and procurements.

Affärsadvokaterna has a long history of providing advice in privacy law. Affärsadvokaterna provides advice to companies in privacy law issues, such as the production of information and agreements texts and the preparation of policy documents. Affärsadvokaterna has wide-ranging experience, and consequently an understanding of a company's special needs with regard to the processing of personal data in their specific business. Affärsadvokaterna has a methodical and pedagogic approach when authority-regulated operational processes are analysed, optimised and implemented. The clients appreciate the fact that the firm combines commitment and dedication with an in-depth understanding of the commercial and technical conditions of the industry. Its background as corporate lawyers combined with its legal experience gives Affärsadvokaterna the opportunity to offer clients focused and cost-efficient management of ongoing legal issues with industry expertise. As a result of the firm's extensive and broad knowledge, Affärsadvokaterna offers cutting-edge legal skills through a combination of commercial awareness, industry knowledge and legal expertise, which results in a business benefit for the client with regard to their use of personal data.

Affärsadvokaterna has a wealth of experience of analysing and implementing business-critical processes for the handling of personal data. The firm is appreciated by its clients for its long history in providing advice in privacy law. Affärsadvokaterna has a very strong focus on the healthcare and IT sector and is assisting both existing and new clients in regards to the General Data Protection Regulation.

Over the years, Affärsadvokaterna has also conducted its own specific examinations and integrity analysis of their clients' handling of personal data and other privacy-sensitive information. Affärsadvokaterna provides companies with tools, in the form of both projects and internal training, in order that, using an integrity analysis, they can analyse and continuously improve the processes that should be used in the challenge of cost-effectively complying with laws and regulations.

More information about cases and major accomplishments can be found at the website [www.affarsadvokaternasverige.se](http://www.affarsadvokaternasverige.se).



# Switzerland

Lorenza Ferrari Hofer



Pestalozzi

Michèle Burnier



## 1 Relevant Legislation and Competent Authorities

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

The Federal Act on Data Protection of 19 June 1992 (the Data Protection Act, the “DPA”) and the Ordinance to the Federal Act on Data Protection of 14 June 1993 (“ODPA”).

Since Switzerland is not a member of the EU, it does not have to comply with the EU General Data Protection Regulation or any other directives applicable in this field.

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

Every Swiss canton has its own data protection statutes with respect to data processing of cantonal public authorities.

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

The Swiss banking secrecy and guidelines thereto impact data protection when bank customer data are processed. Furthermore, secrecy obligations, such as patient secrecy regarding health data as set out in article 321 of the Swiss Criminal Code, have an impact on when respective data are processed. Particular rules concerning data retention and processing also apply in the telecommunication sector.

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

The Federal Data Protection and Information Commissioner (“FDPIC”) is the relevant authority if personal data are processed by federal authorities, individuals and legal entities. The respective Cantonal Data Protection and Information Officer in each canton is the responsible authority if personal data are processed by public authorities of the respective canton.

## 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 (see article 3 lit. a and b DPA).
- **“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 (see article 3 lit. e DPA).
- **“Controller”**  
There is no statutory definition, as the term is not explicitly used in the DPA. The FDPIC defines “Data Controller” or “Data Exporter” in its template outsourcing agreement as follows: the natural or legal person, public authority, agency or any other body established in Switzerland which alone or jointly with others determines the purposes and means of the processing of personal data and which transfers such data (to another country) for the purposes of its processing on his/her behalf.
- **“Processor”**  
There is no statutory definition, as the term is not explicitly used in the DPA. The FDPIC defines “Data Processor” or “Data Importer” in its template outsourcing agreement as follows: natural or legal person, public authority, agency or any other body (established in another country) which agrees to receive personal data from the Data Exporter for the purposes of processing such data on behalf of the latter after the transfer in accordance with his/her instructions.
- **“Data Subject”**  
Natural or legal persons whose data are processed (see article 3 lit. b DPA). It is important to emphasise that the DPA does not only protect personal data of natural persons as most other data protection laws, but also personal data of legal persons.
- **“Sensitive Personal Data”**  
Data on: 1) religious, ideological, political or trade union-related views or activities; 2) health, the intimate sphere or racial origin; 3) social security measures; and 4) administrative or criminal proceedings and sanctions (see article 3 lit. c DPA).

### ■ “Data Breach”

There is no statutory definition, as the term is not explicitly used in the DPA.

### ■ *Other key definitions – please specify (e.g., “Pseudonymous Data”, “Direct Personal Data”, “Indirect Personal Data”)*

#### ■ “Data Owner”

The term used in the DPA is “Controller of the Data File”, which is any private person or federal body that decides on the purpose and content of a data file (see article 3 lit. i DPA).

#### ■ “Pseudonymous Data”

There is no statutory definition. Pseudonymous data are data for which the relation to a natural or legal person is not entirely removed, but rather replaced by a code, which can be attributed based on a specific rule to the respective natural or legal person. Anonymous data are data for which the relation to a natural or legal person is entirely removed.

#### ■ “Personality Profile”

A collection of data that permits an assessment of essential characteristics of the personality of a natural person (see article 3 lit. d DPA).

#### ■ “Data Files”

Any set of personal data that is structured in such a way that the data are accessible by the data subject (see article 3 lit. g DPA).

## 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 as soon as data are processed in Switzerland. Thus, if personal data are archived in Switzerland (e.g., in a cloud), the DPA will apply – even though no data were collected in Switzerland and the data subjects are not located in Switzerland.

## 4 Key Principles

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

#### ■ Transparency

The collection of personal data and in particular the purpose of its processing must be evident to the data subject (see article 4 para. 4 DPA).

#### ■ Lawful basis for processing

Personal data may only be processed lawfully (see article 4 para. 1 DPA).

#### ■ Purpose limitation

Personal data may only be processed for the purpose indicated at the time of collection, that is evident from the circumstances, or that is provided for by law (see article 4 para. 3 DPA).

#### ■ Data minimisation

There is no such principle set out in the DPA, but the FDPIC considers that it is part of the general principle of proportionality.

#### ■ Proportionality

Data processing must be carried out in good faith and must be proportionate (see article 4 para. 2 DPA).

#### ■ Retention

This is not a key principle set out in the DPA. However, the principle of proportionality requires that personal data are only retained as long as it is necessary with respect to the purpose of the data processing. General data retention requirements are not set forth in the DPA, but rather in the Swiss Code of Obligations or sector-specific regulations.

#### ■ *Other key principles – please specify*

There are no other key 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

Any person may request information from the Controller of the Data File as to whether data concerning him/her is being processed (see article 8 para. 1 DPA; exceptions are mentioned in article 9 DPA).

#### ■ Right to rectification of errors

Any data subject may request that incorrect data be corrected (see article 5 para. 2 DPA).

#### ■ Right to deletion/right to be forgotten

Any data subject may request that incorrect data be deleted (see article 5 para. 2 DPA). The right to be forgotten is not explicitly mentioned in the DPA, but the FDPIC and case law consider that such a right results from the general principle of proportionality.

#### ■ Right to object to processing

Data subjects may request (in a civil litigation) that data processing be stopped, that no data be disclosed to third parties, or that the personal data be corrected or destroyed (see article 15 para. 1 DPA). It is important to note that data processing may be blocked by preliminary injunctions.

#### ■ Right to restrict processing

There is no such principle set out in the DPA.

#### ■ Right to data portability

There is no such principle set out in the DPA.

#### ■ Right to withdraw consent

According to article 12 para. 2 lit. b DPA, “anyone must not process data pertaining to a person against that person’s express wish without justification”. Based on this provision, it is possible to withdraw consent at any time.

#### ■ Right to object to marketing

In addition to the objection to data processing for marketing purposes as set out above, there is a special regulation regarding mass emails (i.e., marketing newsletters) in article 3 lit. o of the Unfair Competition Act.

#### ■ Right to complain to the relevant data protection authority(ies)

The FDPIC may investigate cases in more detail on his own initiative or at the request of a third party (see article 29 para. 1 DPA).

#### ■ *Other key rights – please specify*

There are no other key rights.

## 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?

Cross-Border Data Transfer: if personal data are transferred to a country that has no adequate data protection laws in force, additional safeguards are necessary. Safeguards are, for example, data transfer agreements or group-wide data protection policies (for transfers within a group of companies). The FDPIC must be informed about these safeguards prior to transborder disclosure (see article 6 para. 3 DPA and article 6 para. 1 ODPA).

Registration of Data Files with the FDPIC: federal bodies must register their data files with the FDPIC (see article 11a para. 2 DPA). Private persons must register their data files with the FDPIC only if: 1) they regularly process sensitive personal data or personality profiles; or 2) they regularly disclose personal data to third parties (see article 11a para. 3 DPA). Exceptions from the registration duty are set out in article 11a para. 5 DPA and in article 4 ODPA (for example, if the respective legal entity has appointed an internal Data Protection Officer who monitors compliance with data protection laws).

### 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/notification must include both specific but also general information (for further details, see the answer to question 6.5 below).

### 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 the answer to question 6.1 above. The registration of data files is made per data file.

### 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)?

Generally, the local legal entity is the Data Controller who transfers personal data pursuant to the DPA abroad (see the definition in the answer to question 2.1 above) and/or is the Controller of the Data File (see the definition in the answer to question 2.1 above).

Foreign entities domiciled outside of Switzerland may be qualified as Controllers of the Data File in the sense of the DPA. However, the FDPIC is not able and does not enforce the DPA in the case of a foreign legal entity domiciled outside of Switzerland because of the principle of territoriality. In case a foreign legal entity is the Controller of the Data File with personal data of Swiss data subjects, the FDPIC may investigate whether a legal entity in Switzerland is co-controller of the respective data file. The representative or branch office of a foreign Controller of the Data File is not automatically subject to the registration obligation. The representative or branch

office of a foreign entity is usually not to be qualified as Controller of the Data File, since often they do not have the power to decide on the content or purpose of a data file.

### 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)?

Cross-Border Transfers: no detailed information is required if the standard contractual clauses of the EU or the FDPIC are used, but the communication must include the country to which the data will be transferred and the name(s) of the data recipients(s). Otherwise, the copy of the respective contract clauses must be disclosed to the FDPIC.

Data Files: information regarding the notifying entity, contact person for information requests, categories of personal data, categories of data subjects, categories of data recipients, categories of persons having access to the data files and processing purposes must be disclosed. The FDPIC provides a template registration form on its website.

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

Upon complaint, the respective entities or individuals may be fined if they wilfully infringed the registration obligation (see article 34 para. 2 DPA). The fine can be up to CHF 10,000.

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

There is no fee for the registration of data files or cross-border transfer notifications.

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

The registration must be renewed as soon as the notified information changes. There is, however, no strict deadline and the update can be executed electronically.

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

There is no such obligation. Regarding federal and cantonal authorities, such approval obligations may arise out of specific public law.

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

Yes, the notification can be completed online, but the confirmation must be signed by an authorised representative and returned by courier to the FDPIC.

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

Yes, the publicly available list can be accessed via the website of the FDPIC (<https://www.edoeb.admin.ch/edoeb/en/home/data-protection/handel-und-wirtschaft/entreprises/anmeldung-einer-datensammlung.html>).

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

The registration process usually takes between one to two 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?

There are no sanctions.

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

There are no specific provisions in the DPA in this regard; thus, the general rules and principles based on the Swiss Code of Obligations will apply.

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

Yes, a single officer may cover multiple entities.

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

Independence (performs his/her function without instructions from the Controller of the Data File); sufficient resources with respect to skills and time; sufficient personal and organisational power (as he/she must have access to all data files, data processing and information thereto) (see article 12a para. 2 and article 12b para. 2 ODPA).

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

Monitoring the processing of personal data and suggesting corrective measures if data protection regulations should not be complied with, and maintaining a list of all data files (see article 12b para. 1 ODPA).

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

Yes (see article 12a para. 1 lit. b ODPA).

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

No, there is no such requirement under the DPA.

## 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, an agreement with the processor is required.

### 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 not necessarily be in writing, but it must ensure that the data are processed only in the manner permitted for the instructing party itself and is not prohibited by a statutory or contractual duty of confidentiality. In particular, the instructing party must ensure that the processor guarantees data security.

## 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?)

With regard to marketing communications distributed by telephone, email or fax, article 3 lit. u of the Unfair Competition Act prohibits the sending of such communication if the recipient has declared in the official telephone registry that he/she does not wish to receive such communication.

Regarding mass emails and text messages, article 3 lit. o of the Unfair Competition Act requires that such communication is only sent with the prior consent of the recipients and with information on a simple opt-out procedure. An exception is made if the entity received the contact information in connection with the sale of products or services it has purchased before and if the customer was informed at the moment of the data collection about the simple opt-out procedure. In that case, information regarding similar products or services may be sent without prior consent.

### 9.2 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 3 lit. u of the Unfair Competition Act prohibits marketing communication via telephone, email and fax if the recipient has declared in any telephone registry that he/she does not wish to receive such communication. In addition, there are several industry related "do not contact" lists (such as codes of conduct), which many companies respect but which are not mandatory.

### 9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

Yes, they also apply to marketing sent from other jurisdictions.



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

In Switzerland, it is the State Secretariat for Economic Affairs (“SECO”) which is the competent authority to file a claim in case of violation of the interests of many persons (article 10 para. 3 of the Unfair Competition Act). In addition, the FDPIC regularly issues guidelines on data protection aspects of marketing practices.

#### 9.5 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 marketing lists from third parties. The “SDV Schweizer Dialogmarketing Verband” is the leading association regarding dialogue marketing in Switzerland. The association’s members are bound by an ethics code, which is accessible by the public ([http://sdv-konsumenteninfo.ch/selbstregulierung/2012\\_sdv\\_ehrenkodex/](http://sdv-konsumenteninfo.ch/selbstregulierung/2012_sdv_ehrenkodex/)).

#### 9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

In case of intentional misconduct, the respective entity (respectively, the responsible person) may be sanctioned, upon request, with a prison term of up to three years or a monetary penalty of up to CHF 1,080,000 (see article 23 of the Unfair Competition Act). The effective sanctions would, of course, be much lower than the maximum penalties. There is no penalty in case of a negligent misconduct.

### 10 Cookies

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

Swiss law does not require an explicit opt-in regarding cookies. It is sufficient to inform the website users about cookies, the data processed by cookies, the purpose of processing and opt-out mechanisms (see article 45c of the Swiss Telecommunication Act).

#### 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 distinction 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?

No. The FDPIC investigates new trends regarding cookies on a regular basis but has not taken any action, since cookies are not regulated in the DPA.

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

A fine not exceeding CHF 5,000 for non-compliant cookies policy on websites of Swiss providers (see article 53 of the Telecommunication Act).

### 11 Restrictions on International Data Transfers

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

International or cross-border disclosure means any transfer of personal data abroad, including allowing examination (e.g., of an online database), transfer or publication (see article 3 lit. f DPA). Personal data must not be disclosed abroad if the personal integrity of the persons concerned would thereby be seriously harmed (see article 6 para. 1 DPA). A serious violation of personal integrity is assumed if there is no legislation ensuring an adequate level of protection in the country where the data are disclosed.

The conditions covering disclosure of data abroad are applicable irrespective of whether the transfer takes place within the same corporate body or to another legal entity.

#### 11.2 Please describe the mechanisms companies 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 assumption that personal integrity is violated by a disclosure of personal data to a country without appropriate data protection laws can only be refuted if at least one of the minimum conditions stipulated in article 6 para. 2 lit. a to lit. g DPA is present. However, the possibility of justifying the admissibility of the international data transfer based on the general grounds for justification (according to article 13 DPA) is not available.

As a rule of thumb, all countries which have either ratified the ETS 108 agreement or are subject to the EU’s General Data Protection Regulation are considered to have an adequate level of data protection according to Swiss legislation.

In addition, the FDPIC has prepared a non-binding list of those countries whose data protection legislation should ensure appropriate protection.

However, additional precautions according to article 6 para. 2 DPA may be advisable.

The transfer of data abroad within a group of companies is also permissible to countries without an adequate level of data protection, if the companies concerned are subject to group-wide data protection rules which ensure appropriate protection. This regulation privileges international data transfers within a group of companies (article 6 para. 2 lit. g DPA).

Data protection rules which ensure adequate protection must at least contain the elements recommended by the FDPIC for international data transfers, namely:

- list of purposes of use split up according to categories of personal data;
- binding agreement on disclosing data for indicated purposes only;
- protection of the rights of the persons concerned (in particular, rights to information and correction);
- ban on transfer of data to a third party;
- ensuring data security in accordance with the sensitivity of the data; and
- stipulation of compensation liability of the data recipient for violation of contract.

If there are both inadequate legislation in the recipient country as well as insufficient data protection rules within the company, international data transfers among affiliated companies in the group are still permitted, provided one of the minimum requirements of article 6 para. 2 lit. a to f DPA is satisfied:

- sufficient safeguards, in particular contractual clauses, ensure an adequate level of protection abroad;
- the data subject has consented in the specific case;
- the processing is directly connected with the conclusion or the performance of a contract and the personal data are that of a contractual party;
- disclosure is essential in the specific case in order to either safeguard an overriding public interest or for the establishment, exercise or enforcement of legal claims before the courts;
- disclosure is required in the specific case in order to protect the life or the physical integrity of the data subject; or
- the data subject has made the data generally accessible and has not expressly prohibited its processing.

Most legal entities use the EU standard contractual clauses as sufficient safeguards in the sense of article 6 para 2 lit. a DPA. The use of the EU standard contractual clauses also facilitates the notification of the cross-border transfer to the FDPIC (see the answer to question 11.3 below).

### 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 general requirement to register or notify or apply for approval. The FDPIC has to be notified only in two instances:

The FDPIC has to be informed of the fact that adequate contractual guarantees (article 6 para. 2 lit. a DPA) have been concluded or that data protection rules within the group of companies (article 6 para. 2 lit. g DPA) have been implemented. As long as the contractual guarantees are in line with the provisions in the EU standard contractual clauses, the respective data protection agreement does not have to be submitted. The group internal rules also need to be submitted to the FDPIC (article 6 para. 3 DPA and article 6 para. 5 ODPA). In both instances it suffices to inform the FDPIC of the existence of such rules and guarantees. The FDPIC can nevertheless start a data protection compliance review on its own.

## 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 are no specific legislation or provisions under Swiss law on whistle-blowing as such. Any whistle-blower hotlines must, however, comply with the general requirements of the DPA. There are ongoing attempts to regulate whistle-blowing and to provide protection for whistle-blowers. Currently, the protection of the employee as a whistle-blower is very weak. The employee is potentially exposed to civil (e.g., termination of his/her job, potential damages) and criminal (e.g., offences due to false allegations, industrial espionage) sanctions. There are no restrictions as such as to what can be reported to the whistle-blower hotline.

Moreover, there is no duty to notify or register the whistle-blower hotline with the respective authorities. However, collections of sensitive personal data or personality profile must be registered with the FDPIC, even if the persons concerned are aware of the processing. However, if whistle-blower hotlines collect employees' personal data and regularly disclose them to third parties, there is a duty to register. Excluded from this are data collections by companies which have appointed an internal Data Protection Officer (see the answer to question 6.1 above). Swiss doctrine is mainly of the opinion that companies with whistle-blower hotlines do not have to register the respective data collections, because there are usually no sensitive personal data or personality profiles of employees among such data and, even if there is such sensitive personal data, it is not processed on a regular basis.

Whistle-blowing is mainly discussed in Switzerland in connection with the loyalty and confidentiality duties of the employee, the provisions regarding justified termination, and the employer's duty of care towards its employees. The employer must implement all necessary measures in order to ensure that the personality rights of the whistle-blower are not infringed. Accordingly, the employee must be informed transparently and comprehensively about all aspects of the whistle-blower hotline (where it is operated, who is operating it, etc.) and of the consequences his/her whistle-blowing activities may have before using the hotline.

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

There are no provisions prohibiting or discouraging anonymous reporting. In practice, it is, however, often recommended not to report anonymously. The main argument in favour of non-anonymous reports is the transparency principle in article 4 para. 4 DPA (see the answer to question 4.1 above). An employee suspected of misconduct in a whistle-blowing report must be informed about the report, the whistle-blower and the alleged misconduct. It is acceptable to delay informing the suspected employee in order to facilitate investigations.

## 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, there is no general requirement to register/notify or obtain prior approval for the use of CCTV. However, if a CCTV also records activities on public ground (e.g., it records activities on a private parking lot but also covers the nearby public walkway), cantonal or local data protection laws may require separate approval from the cantonal authorities.

As the use of CCTV must be transparent for the persons concerned, they must be informed about the use of CCTV prior to accessing the surveilled premises, e.g., by a visible sign.

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

Yes, the use of CCTV must respect the general principles of the DPA; in particular, the principle of proportionality. Therefore, it is necessary

to weigh up the relevant interests in each case. Further, CCTV by private persons must be strictly limited to their own premises.

## 14 Employee Monitoring

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

In accordance with the DPA and article 328b of the Swiss Code of Obligation, the employee must be previously and transparently informed about the type and method of the electronic monitoring, the scope and period of timeframe of the monitoring and its purpose.

Anonymous monitoring (including monitoring of search strings) of, e.g., employees' use of company-provided information technology according to email and internet user guides or other policies is permissible. Pseudonymous monitoring (i.e., an abbreviation for an employee known only to a very limited group of persons) is only permissible for spot checks. No continuous monitoring is permissible in this case.

In both cases, the employees must be informed of the fact that their information technology use can/will be monitored. They may be informed via monitoring policies.

Systematic and permanent monitoring of the information technology use of specific employees is not permitted, unless: (a) the employee has consented thereto; or (b) if there is no consent, then the following requirements have to be fulfilled: (i) justified suspicion of a criminal offence; (ii) monitoring and reading of emails is necessary to confirm or dispel suspicion; (iii) conserving evidence; and (iv) there is no overriding interest of the employee. If there is an overriding interest, then the consent of the employee must be obtained. Please note that any evidence not collected in compliance with applicable law may not be admissible in court.

Accordingly, the use of so-called spyware, which clandestinely monitors the conduct of a specific employee in the workplace (e.g., computer screen movements), is not permitted and would infringe Swiss law. According to the FDPIC, this also applies to so-called content scanners (if done clandestinely). A content scanner is software that evaluates/scans sent and received emails in accordance with pre-defined keywords and reacts accordingly (cancellation or blocking of emails, etc.).

Clandestine and not pre-announced monitoring is prohibited and cannot be justified by an overriding interest of the employer.

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

See the answer to question 14.1 above: yes, prior transparent information is required; however, consent is generally not necessary.

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

The representatives of the employees in a company have a right to timely and comprehensive information by the company on all matters that allow employees to duly perform their tasks (article 9 of the Federal Act on Information and Participation of Employees in Companies). Since employee monitoring may have an impact on employee performance, employee representatives need to be kept up to date on this subject. However, there is no requirement to consult any entities.

## 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, according to article 7 para. 1 DPA, "personal data must be protected against unauthorised processing through adequate technical and organisational measures".

Moreover, article 8 ODPA provides details on the level of security: anyone who, as a private individual, processes personal data or provides a data communication network shall ensure the confidentiality, availability and integrity of the data in order to ensure an appropriate level of data protection.

- (1) In particular, he/she shall protect the systems against the following risks:
  - a) unauthorised or accidental destruction;
  - b) accidental loss;
  - c) technical faults;
  - d) forgery, theft or unlawful use; and
  - e) unauthorised alteration, copying, access or other unauthorised processing.
- (2) The technical and organisational measures must be adequate. In particular, they must take account of the following criteria:
  - a) the purpose of the data processing;
  - b) the nature and extent of the data processing;
  - c) an assessment of the possible risks to the data subjects; and
  - d) the technological state of the art.
- (3) These measures must be reviewed periodically.

Finally, article 9 ODPA states:

- (1) The Controller of the Data File shall, in particular for automated processing of personal data, take the technical and organisational measures that are suitable for achieving the following goals, in particular:
  - a) entrance control: unauthorised persons must be denied access to facilities in which personal data are being processed;
  - b) personal data carrier control: unauthorised persons must be prevented from reading, copying, altering or removing data carriers;
  - c) transport control: on the disclosure of personal data as well as during the transport of data carriers, the unauthorised reading, copying, alteration or deletion of data must be prevented;
  - d) disclosure control: data recipients to whom personal data are disclosed by means of devices for data transmission must be identifiable;
  - e) storage control: unauthorised storage in the memory as well as the unauthorised knowledge, alteration or deletion of stored personal data must be prevented;
  - f) usage control: the use by unauthorised persons of automated data processing systems by means of devices for data transmission must be prevented;
  - g) access control: the access by authorised persons must be limited to the personal data that they require to fulfil their task; and
  - h) input control: in automated systems, it must be possible to carry out a retrospective examination of what personal data was entered at what time and by which person.

- (2) The data files must be structured in a way that data subjects are able to assert their right of access and their right to have data corrected.

**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) expects voluntary breach reporting.**

No, there is no statutory duty to do so. However, based on the general principles of the DPA, e.g., the transparency principle, it is advisable to notify the data subjects about such a 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) expects voluntary breach reporting.**

See the answer to question 15.2 above.

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

There are no penalties for security breaches in the DPA. If the security breach also represents a breach of an obligation of secrecy, other legislation may be applicable and penalties may apply.

## 16 Enforcement and Sanctions

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

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
Monetary penalty notices	This is not applicable.	This is not applicable.
Recommendations	<p>The FDPIC can investigate cases and request the production of files, obtain information and arrange for processed data to be shown to him.</p> <p>If the investigation reveals that the DPA is being breached by federal bodies, the FDPIC can recommend that the federal body concerned change the method of processing or abandon the processing. The FDPIC informs the department concerned or the Federal Chancellery of his recommendation. If a recommendation is not complied with or is rejected, the FDPIC may refer the matter to the department or to the Federal Chancellery for a decision. The decision is communicated to the data subjects in the form of a ruling.</p> <p>If the FDPIC reveals in an investigation that in the private sector a natural/legal person does not comply with the DPA, it may render recommendations as well. Upon 30 days of the receipt of the recommendation, the legal person must inform the FDPIC on whether it accepts and implements the recommendation or whether it rejects it. In case of a rejection, the FDPIC may bring the case to the Swiss Federal Administrative Court.</p>	This is not applicable.
Enforcement notices	This is not applicable.	This is not applicable.
Prosecution	This is not applicable.	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 FDPIC can issue recommendations regarding the set-up of specific processing activities. These may include the recommendation to ban certain processing activities or to amend a processing activity. If the party concerned does not follow the issued recommendations or rejects them, the FDPIC may involve a federal court. The court's decision will be binding for the parties, subject to appeal to the Federal Supreme Court.

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

The FDPIC issues its recommendations on a regular basis and publishes them on his website (see the answer to question 18.1 below regarding current cases).

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

Yes, the FDPIC also uses its power against companies established in other jurisdictions provided that a predominant connection to Switzerland exists. Based on this principle, the FDPIC, e.g., performed an investigation and issued recommendations in the context of Google Street View against Google, Inc. (together with Google's Swiss subsidiary) as well as in the context of Windows 10 against Microsoft Corporation ([www.edoeb.ch](http://www.edoeb.ch)).

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

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

It depends on whether these requests are made during pending proceedings or outside of such proceedings.

During pending proceedings the companies are not permitted to (directly) respond to such requests. The foreign law enforcement agency must contact the competent Swiss authorities within the international judicial assistance (in civil or criminal matters) system. The Swiss authority then collects and transfers the respective information by way of judicial assistance to the foreign authority. The DPA is not applicable in the case of judicial assistance proceedings (see article 2 para. 2 lit. c DPA).

If a Swiss company is directly approached by a foreign law enforcement agency, the request must be qualified as outside of a pending proceeding and the DPA must be complied with. The legal person may only disclose the information and personal data to the foreign authority if the DPA is complied with, in particular with article 6 DPA regarding cross-border data transfers.

The so-called Swiss blocking statutes (e.g., articles 271 and 273 of the Swiss Criminal Code) are most relevant in this context. Due to the blocking statutes, companies within Switzerland cannot comply with foreign e-discovery requests without incurring the risk of a penal prosecution for unpermitted disclosure. It must be decided on a case-by-case basis whether such requests can be complied with

or whether a specific waiver from the competent authorities must be obtained (if applicable). If a Swiss company violates the blocking statutes, its members of the board might be sanctioned with a fine or imprisonment.

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

The FDPIC has issued a guidance regarding this subject matter. Basically, the guidance comes to the same conclusions as set out in the answer to question 17.1 above.

## 18 Trends and Developments

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

The Swiss Federal Supreme Court dealt with the applicability of data protection issues in international mutual legal assistance in administrative and tax matters. The Swiss Federal Supreme Court ruled that Swiss authorities must take into account the protection of third parties not directly concerned by requests of international mutual legal assistance (such as (former) employees, attorneys, notaries, managers, etc.). Therefore, it is necessary to redact the names of third parties not concerned by the request of international mutual legal assistance. Only if it is necessary to divulge the name in order to comply with the request, a name may be communicated. In tax matters the name may only be disclosed if the name is necessary to clarify the fiscal situation of the taxpayer. Thus, the principle is that the name of third parties not concerned by a request of international mutual legal assistance must not be communicated (Decision 2C\_640/2016 of 18 December 2017). Furthermore, if the name of third parties must be communicated, such third party must be informed about such communication and awarded the status of a party to the proceedings (Decision 2C\_792/2016 of 23 August 2017).

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

The following hot topics are currently a focus:

- Swiss-US Privacy Shield.
- Revision of the DPA.
- Revision of the legal basis for the surveillance by insurers.
- Big Data, in particular for healthcare research and platforms.
- CCTV monitoring.
- Data protection and personalised healthcare.
- Data protection and drones used by individuals for private purposes.
- Dashcams (small video recorders often used in cars).
- Transmission of data to US authorities based on the US Program for Swiss banks (ongoing decisions from the Swiss Federal Supreme Court).

After the European Commission adopted the EU-US Privacy Shield, Switzerland entered into negotiations in order to enter into a similar agreement. In 2017, Switzerland adopted the Swiss-US Privacy Shield (<https://www.edoeb.admin.ch/edoeb/en/home/data-protection/handel-und-wirtschaft/transborder-data-flows/transfer-of-data-to-the-usa.html>).

In September 2017, the Federal Council submitted a draft of the revised DPA to parliamentary discussions, which are currently



ongoing. It is not yet clear when the revised act will come into effect. The goal of this revision is, among others, to strengthen data protection provisions to reflect evolving technological and social circumstances. In this respect, a key objective is to align Swiss data protection laws with European legislation (Regulation (EU) 2016/679 and Directive

2016/680) in order to facilitate continued transborder data flows and to comply with the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention ETS No. 108). Further, companies will be obliged to take steps to prevent potential data breaches whenever personal data are processed.



#### Lorenza Ferrari Hofer

Pestalozzi  
Loewenstrasse 1  
8001 Zurich  
Switzerland

Tel: +41 44 217 92 57  
Email: [lorenza.ferrari@pestalozzilaw.com](mailto:lorenza.ferrari@pestalozzilaw.com)  
URL: [www.pestalozzilaw.com](http://www.pestalozzilaw.com)

Lorenza Ferrari Hofer is head of Pestalozzi's IP&TMT Group and co-head of the Life Sciences Group. She specialises in intellectual property, unfair competition, data law, data protection and contract law. Lorenza Ferrari Hofer has years of experience in structuring complex R&D, know-how transfer and cooperation projects, particularly in the field of life sciences. She assists technology corporations as well as research institutions in both negotiations and strategic matters, and represents them in legal proceedings in front of Swiss courts, arbitral tribunals and regulatory authorities. In addition, Lorenza Ferrari Hofer has a broad knowledge of media, advertising and entertainment matters where she regularly represents and advises companies and individuals in respect of copyright, unfair competition and privacy law issues.

Lorenza Ferrari Hofer regularly lectures and publishes in the fields of international licensing and technology transfer, and in several areas of unfair competition, data protection law and intellectual property law. She is consistently recommended by the leading directories of the legal profession, such as *The Legal 500*, *Chambers & Partners*, *Who's Who Legal*, *WIPR Leaders* and *IAM*.

Her professional languages are German, Italian, English and French.



#### Michèle Burnier

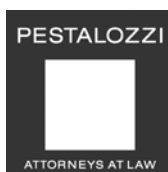
Pestalozzi  
Cours de Rive 13  
1204 Geneva  
Switzerland

Tel: +41 22 999 96 00  
Email: [michele.burnier@pestalozzilaw.com](mailto:michele.burnier@pestalozzilaw.com)  
URL: [www.pestalozzilaw.com](http://www.pestalozzilaw.com)

Michèle Burnier is a partner of Pestalozzi's IP&TMT Group in Geneva. Her fields of expertise include intellectual property, including geographical indications, TRIPS Agreement, unfair competition, data protection, advertising and e-commerce law, IT and telecommunication as well as administrative and contract law. She regularly represents clients before Swiss civil, administrative and/or criminal courts.

She has years of experience in negotiating and drafting complex IP agreements. Michèle Burnier is a member of various national and international organisations, such as AIPPI, INTA, ASA, LIDC and LES (member of the board of the Swiss national group), and she is Chairman of the first Chamber of the Swiss Commission for Fair Advertising (CSL). In addition, Michèle Burnier frequently lectures in seminars in the fields of intellectual property law and unfair competition, also in cooperation with the Swiss Intellectual Property Institute.

Her professional languages are French, German, English and Italian.



Pestalozzi supports international and domestic clients in all aspects of Swiss law from our offices in Zurich and Geneva. The firm is known for integrity, the highest quality standards and proven effectiveness.

Clients benefit from the know-how of over 120 partners, attorneys and support staff. With practice groups and expertise in all areas of business law, Pestalozzi forms customised teams to meet every challenge. Pestalozzi's contacts include an international network of lawyers who give you access to top-quality law firms in jurisdictions worldwide.

The care of clients is the focus of everything we do at Pestalozzi, supported by the diversity of our people and a dynamic company culture that ensures a creative, practical and effective response in every case.

Pestalozzi's main clients are large domestic and foreign corporations. We also assist medium-sized companies and private individuals. The broad range of sectors it serves includes financial services as well as a vast array of industries ranging from automobiles to watches.

# Taiwan

Lawrence Ong



Kelvin Chung



KPMG Law Firm

## 1 Relevant Legislation and Competent Authorities

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

Personal Information Protection Act (hereinafter, “PIPA”).

### 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?

Yes, there are some sector-specific laws that may impact data protection, especially financial regulations.

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

The Ministry of Justice is responsible for interpreting PIPA. Data protection of each sector shall be governed by the government authority in charge of the specific industry at the central government level and municipality.

## 2 Definitions

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

#### ■ “Personal Data”

According to Item 1 of Article 2 of PIPA, “Personal Data” means the name, date of birth, I.D. card number, passport number, characteristics, fingerprints, marital status, family, education, occupation, medical record, medical treatment, genetic information, sexual life, health examination, criminal record, contact information, financial conditions, social activities and other information which may be used to identify a natural person, whether directly or indirectly.

#### ■ “Processing”

According to Item 4 of Article 2 of PIPA, “Processing” means to record, input, store, compile, correct, duplicate, retrieve, delete, output, connect or internally transmit information for the purpose of establishing or using a personal data file.

#### ■ “Controller”

There is no specific definition.

#### ■ “Processor”

According to Article 4 of PIPA, “Processor” means one who is commissioned by a government agency or non-government agency to collect, process or use personal data.

#### ■ “Data Subject”

According to Item 9 of Article 2 of PIPA, “Data Subject” means an individual whom which personal data has been collected, processed or used from in accordance with PIPA.

#### ■ “Sensitive Personal Data”

According to Article 6 of PIPA, “Sensitive Personal Data” means medical records, medical treatment, genetic information, sexual life, health examination and criminal records.

#### ■ “Data Breach”

According to Article 12 of PIPA, “Data Breach” means the situation where personal data is stolen, disclosed, altered or infringed due to a violation of PIPA.

#### ■ Other key definitions – please specify (e.g., “Pseudonymous Data”, “Direct Personal Data”, “Indirect Personal Data”)

“Collection” means to collect personal data in any form and way.

“Use” means all methods of personal data use other than processing.

“International Transmission” means the cross-border processing or use 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?

Yes, when they collect, process or use personal data of citizens of the Republic of China outside the territory of the Republic of China.

## 4 Key Principles

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

#### ■ Transparency

According to Paragraph 1 of Article 8 of PIPA, an individual should be precisely notified of the following items:

1. the name of the government agency or the non-government agency;
2. purpose of collection;
3. classification of the personal data;
4. time period, area, target and usage method of personal data;
5. rights of the data subject and ways to exercise them as prescribed in Article 3 of PIPA; and
6. the influence on his rights and interests if the data subject chooses not to provide his personal data.

#### ■ Lawful basis for processing

A government agency should ensure compliance with one of the following conditions when collecting personal data:

1. it is within the scope of its job functions provided by laws and regulations;
2. consent has been given by the data subject; or
3. the rights and interests of the data subject will not be harmed.

A non-government agency should ensure compliance with one of the following conditions when collecting personal data:

1. ensure that it is in accordance with laws;
2. there is a contractual or quasi-contractual relationship between the parties and proper security measures have been adopted;
3. the data subject has made public such information by himself or if the information has been publicised legally;
4. it is necessary for public interests on statistics or for academic research purposes conducted by a research institution. The information may not lead to the identification of a specific person after its processing by the provider or from the disclosure by the collector;
5. consent has been given by the data subject;
6. it is necessary to promote public interests;
7. the personal data is obtained from publicly available resources. However, it is exempted if processing and usage of the data is limited by the data subject and the interests of the data subject should be protected; or
8. the rights and interests of the data subject are not harmed.

#### ■ Purpose limitation

Yes, according to Article 5 of PIPA, collection of personal data should not go beyond the purpose of collection and should be reasonable and fair.

#### ■ Data minimisation

Collecting, processing or using personal data should not go beyond the purpose of collection.

#### ■ Proportionality

Yes, according to Article 5 of PIPA, collection of personal data should not go beyond the purpose of collection and should be reasonable and fair.

#### ■ Retention

The data collected should be deleted when the specific purpose no longer exists or if the time period expires, unless

it is necessary for the performance of an official duty or fulfilment of a legal obligation or when it is agreed by the data subject in writing.

#### ■ Other key principles – please specify

The information should be handled in accordance with the principle of *bona fide*.

## 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

Yes, according to Item 1 of Article 3 of PIPA, data subjects have the right to inquire and request for a review of their personal data. According to Article 10 of PIPA, upon the request of the data subject, the government agency or non-government agency should respond to the inquiry, offer a review or provide a copy of the personal data collected.

#### ■ Right to rectification of errors

Yes, according to Item 3 of Article 3 of PIPA, data subjects have the right to request for supplementation or correction of their personal data. According to Paragraph 1 of Article 11 of PIPA, the government agency or the non-government agency should ensure the accuracy of personal data, and correct or supplement it *ex officio* or upon the request of the data subject.

#### ■ Right to deletion/right to be forgotten

Yes, according to Item 5 of Article 3 of PIPA, data subjects have the right to request for the deletion of their personal data. According to Paragraphs 3 and 4 of Article 11 of PIPA, the information collected should be deleted, ceased to be processed or used *ex officio* or upon the request of the data subject when the specific purpose no longer exists or when the time period expires. The information collected should be deleted, ceased to be processed or used *ex officio* or upon the request of the data subject in cases where a violation of PIPA has occurred during the collection, processing or usage of that information.

#### ■ Right to object to processing

Yes, according to Item 4 of Article 3 of PIPA, data subjects have the right to request for discontinuation of the collection, processing or usage of their personal data. According to Paragraphs 2, 3 and 4 of Article 11 of PIPA, in the event of a dispute regarding the accuracy of personal data, its processing or use shall be ceased voluntarily or upon the request of the data subject. The data collected should be deleted, ceased to be processed or used *ex officio* or upon the request of the data subject when the specific purpose no longer exists or when the time period expires, unless it is necessary for the performance of an official duty or fulfilment of a legal obligation or when it is agreed by the data subject in writing. In addition, the data collected should be deleted, ceased to be processed or used *ex officio* or upon the request of the data subject in cases where a violation of PIPA has occurred during the collection, processing or usage of that data.

#### ■ Right to restrict processing

There are no rights in relation to restricting processing.

#### ■ Right to data portability

There is no right to data portability.

#### ■ Right to withdraw consent

Not specified in PIPA.

#### ■ Right to object to marketing

Yes, according to Paragraph 2 of Article 20 of PIPA, when a

non-government agency uses personal data for the purpose of marketing and the data subject has refused to such, the agency should stop its actions. The non-government agency should notify the data subject of the ways to refuse marketing when it first performs marketing acts and should pay necessary fees.

■ **Right to complain to the relevant data protection authority(ies)**

The individual may notify relevant data protection authorities of PIPA violations. However, the data protection authorities are not obliged to respond.

■ *Other key rights – please specify*

There are no other key rights.

## 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 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?

This is not applicable in our jurisdiction.

### 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.

There are no requirements or options to appoint a Data Protection Officer under PIPA. Although, according to Article 18 of PIPA, the government agency which keeps personal data files should assign personnel for security and maintenance of those files to prevent them from being stolen, altered, damaged, destroyed or disclosed. However, such personnel are not the same as a Data Protection Officer in the European context.

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

This is not applicable in our jurisdiction.

### 7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect to 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?**

No, they do not have to enter into any form of 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.)?**

It is not necessary to enter into an 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?)**

Not specified under PIPA.

**9.2 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 Paragraphs 2 and 3 of Article 20 of PIPA, when a non-government agency uses personal data for the purpose of marketing and such has been refused by the data subject, the agency should stop its actions. The non-government agency should notify the data subject of the ways to refuse marketing when it first performs marketing acts and should pay the necessary fees.

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

Not specified under PIPA.

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

Yes, the Financial Supervisory Commission.

**9.5 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 lawful to purchase marketing lists from third parties.

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

An administrative fine of no less than NT\$20,000 but no more than NT\$200,000 should be imposed upon each instance of a breach.

## 10 Cookies

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

This is not specified under PIPA.

**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 have not.

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

There are no such penalties.

## 11 Restrictions on International Data Transfers

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

According to Article 21 of PIPA, the government authority in charge of the specific industry may limit its action if one of the following occurs when the non-government agency transmits personal data internationally:

1. where it involves major national interests;
2. where a national treaty or agreement specifies otherwise;
3. where the country receiving personal data lacks proper regulations to protect personal data and it might harm the rights and interests of the data subject; or



4. where international transmission of personal data is made indirectly in which the provisions of PIPA may not be applicable.

For example, telecommunication carriers shall not transmit personal data to China.

**11.2 Please describe the mechanisms companies 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.).**

Generally, companies may transfer personal data freely unless authorities state otherwise.

**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, they do not.

## 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 are no mandatory rules to regulate whistle-blowers in Taiwan.

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

This is not applicable in our jurisdiction.

## 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. In addition, according to Item 2 of Paragraph 1 of Article 51 of PIPA, the provisions of PIPA are not applicable under the following situations: if audio-visual information is collected, processed or used in public places or for public activities and are not associated with other personal data.

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

No, there are no limits.

## 14 Employee Monitoring

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

There are no specific requirements on the monitoring of employees under PIPA. However, according to Taiwan High Court's decision in 2013, employers are allowed to monitor the employees' performance in order to protect the employers' assets and execute their supervising power. However, employers shall not abuse their power. They shall apply the principle of proportionality when monitoring employees. In addition, the "reasonable expectation of privacy test" disclosed in Judicial Yuan Interpretation No. 689 should also be emphasised in the employee monitoring.

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

This is not specified in the court's decision.

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

They do not need 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, according to Article 18 of PIPA, a government agency which keeps personal data files should assign personnel for security and maintenance of those files to prevent them from being stolen, altered, damaged, destroyed or disclosed. According to Paragraph 1 of Article 27 of PIPA, the non-government agency which keeps personal data files should adopt proper security measures to prevent them from being stolen, altered, damaged, destroyed or disclosed. Controllers and processors are responsible for ensuring that data are kept secure.

In addition, according to Article 12 of Enforcement Rules of PIPA, proper security measures shall mean the technical or organisational measures taken by the government agency or the non-government agency for the purpose of preventing personal data from being stolen, altered, damaged, destroyed or disclosed.

The measures prescribed in the preceding paragraph may include the following matters and shall act in accordance with the principle of proportionality to achieve the personal data protection objective:

1. allocating management personnel and substantial resources;
2. defining the scope of personal data;
3. establishing the mechanism for risk evaluation and management of personal data;
4. establishing the mechanism for preventing, giving notice of, and responding to accidents;
5. establishing an internal management procedure for collecting, processing and using personal data;

6. managing information security and personnel;
7. promoting acknowledgment, education and training;
8. managing the security of the facility;
9. establishing a mechanism of auditing information security;
10. keeping records on the use, locus information and proof; and
11. integrating continuous improvements on the security and maintenance 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) expects voluntary breach reporting.**

No, there is not.

**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) expects voluntary breach reporting.**

Yes, according to Article 12 of PIPA, when personal data is stolen, disclosed, altered or infringed in other ways due to a violation of PIPA, the government agency or non-government agency should notify the data subject after an inspection. According to Paragraph 1 of Article 22 of the Enforcement Rules of PIPA, the contents of the “notification to the data subject” referred to in Article 12 of PIPA shall include the fact that personal data has been infringed and the responding measures taken.

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

A person who intends to make unlawful profits for himself or for a third data subject, or intends to infringe upon the interests of others by illegally changing or deleting personal data files, or by other illegal means, and has impeded the accuracy of another person’s personal data files and caused damage to others should be imprisoned or held in custody for no more than five years or fined no more than NT\$1,000,000, or both. According to Article 44 of PIPA, a government official who takes advantage of his position or opportunity or means available to him to commit the offences should be subject to punishments half as severe as those enumerated above.

As for the civil compensation responsibility, according to Article 29 of PIPA, with regard to damages caused to multiparties by the same cause and fact, the total amount of compensation should not exceed NT\$200,000,000. However, if the interests involved are over the amount in the preceding sentence, the amount of interests should be set as the limit.

## 16 Enforcement and Sanctions

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

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
The government authority in charge of a specific industry at the central government level, municipality directly under the central government, or county or city government may perform an inspection (by staff who carry badges), if it is necessary for the protection of personal data, the disposal after termination of business, the limitation of international transmission, other routine examinations or if PIPA may be violated.	The government authority may detain or duplicate the personal data or its files which may be confiscated or may be served as evidence. The owner, holder or keeper of those objects should offer them upon request. A compulsory enforcement that might harm the rights of the non-government agency the least may be applied to refusals without proper reasons.	None.
	For a non-government agency that violates the provisions of PIPA, one of the following actions may be ordered jointly with a fine, as regulated by the government authority: 1. to forbid the collecting, processing or usage of the personal data; 2. to demand the erasure of the personal data files already processed; 3. to confiscate or to destroy the personal data illegally collected; or 4. to publicise the violation, the name of the non-government agency and the name of the person in charge.	
	The government authority may order the non-government agency to take corrective measures within a specified time period. If they are not taken within that period, an administrative fine of no less than NT\$20,000 but no more than NT\$200,000 should be imposed upon the agency for each violation.	

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
	The non-government agency that evades, obstructs or refuses entry, inspection or the measures adopted by the government authority without proper reasons should be imposed an administrative fine of no less than NT\$20,000 by the government authority.	

### 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?

There is no single and specific data protection authority in Taiwan. However, the government authority in charge of the specific industry at the central government level, municipality directly under the central government, or county or city government may forbid the collecting, processing or usage of the personal data.

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 government authority in charge of the data subject's industry at the central government level, municipality directly under the central government, or county or city government may perform an inspection (by staff who carry badges), if it is necessary for the protection of personal data, the disposal after termination of business, the limitation of international transmission, other routine examinations or if PIPA may be violated.

The Financial Examination Bureau of FSC (Financial Supervisory Commission) performs financial inspections routinely, and a data protection inspection is also included. According to the inspection result of 2017 released by the FSC, the most common deficiency includes non-performance of personal data mapping and risk analysis.

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

No, never.

## 17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

### 17.1 How do companies typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

If companies would like to provide personal data to foreign law enforcement agencies, the requirements listed in Article 19 or 20 of PIPA should be met.

According to Article 19, the non-government agency should not process personal data unless there is a specific purpose and in compliance with the following conditions:

1. it is in accordance with laws;
2. there is a contractual or quasi-contractual relationship with the data subject and proper security measures have been adopted;
3. the data subject has made public such information by himself /herself or when the information has been publicised legally;
4. it is necessary for public interests on statistics or for academic research purposes conducted by a research institution. The information may not lead to the identification of a specific person after its processing by the provider or from the disclosure by the collector;
5. consent has been given by the data subject;
6. it is necessary to promote public interests;
7. the personal data is obtained from publicly available resources. However, it is exempted if the processing or usage of the information is limited by the data subject and the interests of the data subject should be protected; and
8. the rights and interests of the data subject are not harmed.

According to Article 20, the non-government agency should use the personal data in accordance with the scope of the specific purpose of collection provided. However, the information may be used outside this scope upon the occurrence of one of the following conditions:

1. it is in accordance with laws;
2. it is necessary to promote public interests;
3. it is to prevent harm on the life, body, freedom or property of the data subject;
4. it is to prevent harm on the rights and interests of other people;
5. it is necessary for public interests on statistics or the purpose of academic research conducted by a government agency or an academic research institution, respectively. The information may not lead to the identification of a specific person after its processing by the provider, or from the disclosure by the collector;
6. consent has been given by the data subject; or
7. such use benefits the data subject.

Generally speaking, the companies would try to obtain consent from data subjects in advance or afterwards. In addition, foreign law enforcement agencies may seek assistance from local law enforcement agencies. For example, foreign courts may seek the assistance of local courts though foreign affairs authorities under the "Law in Supporting Foreign Courts on Consigned Cases" to investigate the evidence of civil or criminal cases. In such circumstances, there is no doubt that the requirement of "it is in accordance with law" is fulfilled.

### 17.2 What guidance has/have the data protection authority(ies) issued?

None has been issued.

## 18 Trends and Developments

### 18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

A government body may process or use the personal data for the purpose of carrying out its functional duty. According to a verdict of the Supreme Administrative Court released on January 2017, the court decided that the Ministry of Health and Welfare's act of

establishing the National Health Insurance Database was considered as exercising its legal duty under the Organic Act for Ministry of Health and Welfare. In other words, “it is within the scope of job functions provided by laws and regulations”. Therefore, the Ministry of Health and Welfare possessed the legal basis to process/use the citizen’s personal data to build the database. In addition, the verdict was not in favour of the plaintiff’s request to opt-out from this specific process. This controversial judgment has been highly criticised by human rights groups. Currently, this case is under constitutional review by the Grand Justices of the Judicial Yuan.

## 18.2 What “hot topics” are currently a focus for the data protection regulator?

The interaction between privacy rights and big data has become a hot topic recently. The most highly debated issue is whether companies or governmental bodies which collect personal data can transform them into de-identification information as big data and perform analysis, and whether the data subject has the right to opt-out from this process.



### Lawrence Ong

KPMG Law Firm  
61F, No. 7, Sec. 5, Xinyi Road  
Taipei City 11049  
Taiwan

Tel: +886 2 2728 9696  
Email: [lawrence.ong@kpmg.com.tw](mailto:lawrence.ong@kpmg.com.tw)  
URL: [www.kpmg.com.tw/law](http://www.kpmg.com.tw/law)

Lawrence is the Executive Consultant of KPMG Law Firm, focusing his practice on technology law, data protection, and mergers and acquisitions.



### Kelvin Chung

KPMG Law Firm  
61F, No. 7, Sec. 5, Xinyi Road  
Taipei City 11049  
Taiwan

Tel: +886 2 2728 9696  
Email: [kelvinchung1@kpmg.com.tw](mailto:kelvinchung1@kpmg.com.tw)  
URL: [www.kpmg.com.tw/law](http://www.kpmg.com.tw/law)

Kelvin is Senior Attorney of KPMG Law Firm, focusing his practice on technology law, data protection, and civil and administrative litigation.



One of Taiwan's premier full-service law firms, KPMG Law Firm forges close strategic alliances with the accounting, tax, financial advisory, and information technology advisory arms of KPMG in Taiwan. As an integrated service team, KPMG Law Firm provides market-leading practices and expertise for many industry sectors, and consistently offers commercially useful integrated legal advice that will assist clients to successfully compete in today's ever-changing global market. Clients' challenges are the key driver to KPMG Law Firm's innovation.

Globally, KPMG law firms have more than 1,500 lawyers in 74 jurisdictions around the world, supported by KPMG's global network of over 190,000 multidisciplinary professionals in 155 offices.

# Turkey

Elvan Sevi Fırat



Fırat İzgi Attorney Partnership

Doğukan Doru Alkan



## 1 Relevant Legislation and Competent Authorities

### 1.1 What is the principal data protection legislation?

The principal data protection legislation is the newly enacted **Law on the Protection of Personal Data** numbered 6698, namely **KVKK**, along with its secondary legislation which currently consists of: **the Regulation on Personal Data Protection Experts** which has entered into force after its promulgation in the Official Gazette on 9 February 2018; **the Regulation on the Data Controllers Registry** which was promulgated in the last days of 2017 in the Official Gazette dated 30 December 2017; **the Regulation Concerning Working Rules and Procedures of the Personal Data Protection Board** which came into force with its promulgation in the Official Gazette on 16 November 2017; and **the Regulation on the Erasure, Destruction or Anonymization of Personal Data** which was promulgated in the Official Gazette of 28 October 2017.

### 1.2 Is there any other general legislation that impacts data protection?

The data protection concept has recently gained popularity in Turkey, since KVKK, inspired by the famous EU Directive numbered. 95/46/EC (“**Directive**”), was enacted on 7 April 2016. KVKK has significant similarities with the Directive as it is prepared based on the Directive. KVKK is the first law which specifically regulates the protection of personal data. Before the enactment of KVKK, there were some provisions concerning data protection in several regulations regarding certain regulated sectors. These provisions, all of which take their sources from a single provision in the Turkish Constitution which regulates the right to privacy and data protection, and a few provisions in the Turkish Penal Code regulating the unlawful recording, acquisition or dissemination of personal data, along with a provision regarding the protection of personality in the Turkish Civil Code, were not adequate in terms of satisfying the needs of today’s technology and the increasing volume of personal data processing.

### 1.3 Is there any sector-specific legislation that impacts data protection?

There are several sector-specific laws and regulations that impact data protection including:

- Law on the Regulation of Electronic Commerce numbered 6563.
- The Regulation on Distance Contracts.

- Law on Regulating Broadcasting in the Internet and Fighting against Crimes Committed through Internet Broadcasting numbered 5651.
- Banking Law numbered 5411.
- Electronic Communications Law numbered 5809.
- Law on Payment and Security Reconciliation Systems Payment Services and Electronic Money Organisations numbered 6493.
- Regulation on Internal Systems on Banks and Capital Sufficiency Evaluation Process.
- Regulation on Patient Rights.
- Regulation on Protection and Privacy of Personal Health Data.

### 1.4 What authority(ies) are responsible for data protection?

The national Data Protection Authority is the Personal Data Protection Authority. The Authority’s decision-making body is the Personal Data Protection Board, whose duties and powers are regulated under the Regulation on the Working Procedures and Principles of Personal Data Protection Board.

## 2 Definitions

### 2.1 Please provide the key definitions used in the relevant legislation:

- **“Personal Data”**  
As per KVKK, personal data is defined as all the information relating to an identified or identifiable natural person.
- **“Processing”**  
As per KVKK, processing of personal data means any operation performed upon personal data, such as the collection, recording, storage, retention, alteration, re-organisation, disclosure, transferring, taking over, making retrievable, classification or preventing the use thereof, fully or partially through automatic means or provided that the process is a part of any data registry system, through non-automatic means.
- **“Controller”**  
As per KVKK, the Data Controller means a natural or legal person who determines the purpose and means of processing personal data and is responsible for establishing and managing the data registry system.
- **“Processor”**  
Pursuant to KVKK, the processor means the natural or



legal person who processes personal data on behalf of the controller upon his authorisation.

- **“Data Subject”**  
As per KVKK, data subject is defined as the natural person whose personal data is processed.
- **“Sensitive Personal Data”**  
The term used in KVKK corresponding to Sensitive Personal Data is **Personal Data of Special Nature**. As per KVKK, personal data relating to the race, ethnic origin, political opinion, philosophical belief, religion, sect or other belief, clothing, membership to associations, foundations or trade unions, health, sexual life, convictions and security measures, and biometric and genetic data are deemed to be personal data of a special nature.
- **“Data Breach”**  
A data breach means any kind of data processing that violates the provisions stipulated under KVKK.
- **Other key definitions – please specify (e.g., “Pseudonymous Data”, “Direct Personal Data”, “Indirect Personal Data”)**
  - **“Explicit Consent”**  
As per KVKK, explicit consent is defined as freely given, specific and informed consent.
  - **“Anonymising”**  
As per KVKK, anonymising is defined as rendering personal data impossible to link with an identified or identifiable natural person, even through matching them with other data.
  - **“Data Registry System”**  
As per KVKK the data registry system is defined as the registry system for personal data, registered after being structured according to certain criteria.

### 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 obligations of Data Controllers are stipulated under KVKK without making any exceptions. Therefore, any legal or natural person processing personal data in Turkey who determines the purpose and means of processing personal data and is responsible for establishing and managing the data registry system shall be subject to those laws and regulations. In addition to that, as per KVKK, the relevant provisions of Turkish Penal Code numbered 5237 shall apply in terms of the crimes concerning personal data. In terms of the Turkish Penal Code, the territoriality principle shall be applied. Therefore, Turkey may prosecute criminal offences that are committed within its borders. In this respect, businesses established in other jurisdictions might be subject to those laws regarding their offences committed within Turkish borders.

### 4 Key Principles

#### 4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**  
The whole process, purpose and the scope of data processing must be clear, well informed and easy to understand. The

personal data must be processed in a transparent manner in relation to the data subject.

- **Lawful basis for processing**  
The processing of personal data must be lawful and in conformity with rules of *bona fides*.
- **Purpose limitation**  
The data must be processed for specific, explicit and legitimate purposes.
- **Data minimisation**  
The processing of data must be relevant, limited and necessary for carrying out the purpose for which the data is processed.
- **Proportionality**  
The processing of data must be proportionate to the purposes for which they are processed.
- **Retention**  
The personal data must be retained for the period of time stipulated by relevant legislation, or the purpose for which they 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 of access to data/copies of data**  
Each person has the right to apply to the controller and to learn whether his personal data are processed or not, to request information if his personal data are processed and to learn the purpose of his data processing and whether this data is used for the intended purposes.
- **Right to rectification of errors**  
Each person has the right to apply to the controller and to request the rectification of the incomplete or inaccurate data, if any.
- **Right to deletion/right to be forgotten**  
Each person has the right to apply to the controller and to request the erasure or destruction of his personal data.
- **Right to object to processing**  
Each person has the right to apply to the controller and to object to the processing, exclusively by automatic means, of his personal data, which leads to an unfavourable consequence for the data subject and also to request compensation for the damage arising from the unlawful processing of his personal data.
- **Right to restrict processing**  
Right to restrict processing is not specifically mentioned under KVKK; however, as per the guidelines and Q&A's published by the Data Protection Authority, each person has the right to restrict processing regarding his personal data.
- **Right to data portability**  
Not specifically regulated under the Turkish data protection legislation.
- **Right to withdraw consent**  
Each data subject has the right to proactively withdraw his consent.
- **Right to object to marketing**  
In comparison with the GDPR, KVKK and its secondary legislation does not specifically mention right to object to marketing; however, as per KVKK, each data subject may already object to or restrict any kind of processing or withdraw his previous consent.

## ■ Right to complain to the relevant data protection authority(ies)

If the application to the Data Controller 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 within 30 days when he learns about the response of the controller, or within 60 days as of the application date, in any case. However, a complaint cannot be filed before exhausting the remedy of application to the controller.

## 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?

As per Article 16 of KVKK, natural or legal persons who process personal data are obliged to enrol in the Registry of Data Controllers before proceeding with data processing. However, by taking into account the objective criteria set by the Turkish Data Protection Board such as the nature and quantity of the data processed, the legal requirement for data processing, or transferring the data to third parties, the Board may provide exception to the obligation of enrolment in the Registry of Data Controllers.

### 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)?

Application for enrolling in the Registry of Data Controllers shall be made with a specific notification including but not limited to the list of all processing activities along with data categories and purposes, security measures and retention periods. Please see also question 6.5 below for more detailed information.

### 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 shall be made per Data Controller. Please see our answer to question 6.5 below for the information to be provided by controllers during the registration.

### 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 natural or legal person processing personal data in Turkey who determines the purpose and means of processing personal data and is responsible for establishing and managing the data registry system must notify the Data Protection Authority via the Data Controllers Registry Information System (“**VERBİS**”).

### 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)?

Pursuant to KVKK, the information to be provided by controllers during the registration is as follows:

- Identity and address of the controller and of his representative, if any.
- Purposes for which the personal data will be processed.
- Explanations about group(s) of personal data subjects as well as about the data categories belonging to these people.
- Recipients or groups of recipients to whom the personal data may be transferred.
- Personal data which is envisaged to be transferred abroad.
- Measures taken for the security of personal data.
- Maximum period of time required for the purpose of the processing of personal data.

### 6.6 What are the sanctions for failure to register/notify where required?

Those who fail to meet the obligations for enrolling in the Registry of Data Controllers and making a notification as provided for in Article 16 of KVKK shall be required to pay an administrative fine of **TL 20,000 to TL 1,000,000**.

### 6.7 What is the fee per registration/notification (if applicable)?

Although there was a registration fee envisaged in the government proposal for the registration to the Registry, this provision has been taken out before the enactment of KVKK. The registration to the Registry is free of charge.

### 6.8 How frequently must registrations/notifications be renewed (if applicable)?

Not applicable. However, any changes regarding the information given to the Registry during the registration process shall be promptly notified to the Authority.

### 6.9 Is any prior approval required from the data protection regulator?

Prior approval is not required. However it is worth noting that, by taking into account the objective criteria set by the Board such as the nature and quantity of the data processed, the legal requirement for data processing, or transferring the data to third parties, the Board may provide exception to the obligation of enrolment in the Registry.

### 6.10 Can the registration/notification be completed online?

As per the Regulation on the Data Controllers Registry, all transactions related to the registry will be carried out by Data Controllers via **VERBİS**. Data Controllers will have to enrol in the registry before processing personal data. The Personal Data Protection Authority

announced on its website that registration obligation for Data Controllers will begin right after the VERBİS is put into service and a beginning date is determined by the Data Protection Board.

#### **6.11 Is there a publicly available list of completed registrations/notifications?**

Yes, there will be a publicly available list of completed registrations. The publicly available list in the Registry includes the identity of the Data Controller, their representative, their address and registered e-mail address, the purposes of processing along with the data categories, security measures, retention period and information on the transfer of data.

#### **6.12 How long does a typical registration/notification process take?**

The beginning date of the VERBİS system is yet to be determined by the Data Protection Board. Therefore, the duration of the registration process is unknown.

### **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 as it is not specifically mentioned in KVKK (in opposition to the GDPR). However, appointing a Data Protection Officer who will oversee the responsibilities of controllers is highly recommended as it may prevent controllers from overlooking obligations set forth under the data protection legislation.

#### **7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?**

This is not applicable in Turkey.

#### **7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect to his or her role as a Data Protection Officer?**

This is not applicable in Turkey.

#### **7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?**

This is not applicable in Turkey.

#### **7.5 Please describe any specific qualifications for the Data Protection Officer required by law.**

This is not applicable in Turkey.

#### **7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?**

This is not applicable in Turkey.

#### **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 Turkey.

#### **7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?**

This is not applicable in Turkey.

### **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?**

KVKK and its secondary legislation does not specifically mention a necessity of an agreement between the processor and the controller.

#### **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 mentioned above, entering into an agreement is not necessary. In that regard, there is no formality regarding such an agreement. However, the processors already have obligations arising from KVKK itself. The processor must process personal data on behalf of the controller upon his authorisation and in line with his instructions. The processor is also obliged to keep personal data secure and private, and to not disclose the personal data that he has learned to anyone in breach of KVKK.

### **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 Law on Regulation of Electronic Commerce numbered 6563 stipulates that data subjects must opt in to receiving marketing communications. However, as an exemption, marketing communications can be sent to tradesmen and merchants without obtaining opt-in consent. Furthermore, an opt-out must be provided in the marketing communications and the data subject must be able to use this right at any time without any justification.

#### **9.2 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 will fall under the Law on Regulation of Electronic Commerce numbered 6563; however, marketing through physical means does not fall under the Law numbered 6563. Therefore, general provisions of KVKK shall be applied.

### 9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

The Law on Regulation of Electronic Commerce does not make any differentiation in terms of jurisdictions. Therefore, should the effects of such marketing take place within Turkish borders, the restrictions stipulated by the Law on Regulation of Electronic Commerce shall be applied.

### 9.4 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

Currently, there is no enforcement action taken by the Authority against breaches of marketing restrictions.

### 9.5 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 specific rule mentioning marketing lists in Turkish laws and regulations. However, general provisions of KVKK shall be applied. Selling and purchasing marketing lists shall be deemed as transfer of data to third parties, and therefore requires the explicit consent of the data subjects.

### 9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

The penalties for sending marketing communications in breach of the applicable restrictions set forth by the Law numbered 6563 mentioned above range from TL 1,000 to TL 20,000. Should the marketing communications be sent to multiple recipients at once, the fines may be multiplied by up to 10.

## 10 Cookies

### 10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

There is no specific law or regulation in Turkey in relation to cookies. Therefore, general principles and provisions of KVKK shall be applied in matters regarding cookies or similar technologies.

### 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 Turkey.

### 10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

The Authority has neither taken any action nor provided any guidance regarding cookies.

### 10.4 What are the maximum penalties for breaches of applicable cookie restrictions?

There are no cookie-specific restrictions in Turkish laws and regulations. Please see section 16 for administrative sanctions.

## 11 Restrictions on International Data Transfers

### 11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

Pursuant to article 9 of KVKK, personal data cannot be transferred abroad without explicit consent of the data subject.

### 11.2 Please describe the mechanisms companies 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 that companies typically use to transfer personal data is the consent of the data subject by virtue of the fact that it is procedurally easy. Adding clauses to the consent forms covering the transfer of personal data abroad is currently the most efficient way to transfer 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.

Personal data may be transferred abroad without explicit consent of the data subject, provided that one of the conditions set forth in Articles 5 and 6 of KVKK exist and that:

- Sufficient protection is provided in the foreign country where the data is to be transferred.
- The controllers in Turkey and in the related foreign country guarantee a sufficient protection in writing and the Board has authorised such transfer, where sufficient protection is not provided.

The countries where a sufficient level of protection is provided are yet to be determined and announced by the Board. Furthermore, in cases where the interest of Turkey or the data subject will seriously be harmed, personal data, without prejudice to the provisions of international agreements, may only be transferred abroad upon the Board's permission after receiving the opinions of related public institutions and organisations.

## 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 are not specifically regulated under Turkish laws and regulations. Therefore, general provisions of the relevant laws shall be applied in matters related to these hotlines. The personal data collected through these hotlines should be handled by controllers in line with the principles and obligations set forth by KVKK.



**12.2 Is anonymous reporting prohibited, or strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do companies typically address this issue?**

Please see 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)?**

Since there is no specific provision regarding the use of CCTV in the Turkish data protection legislation, general provisions shall apply to the use of CCTV; therefore, CCTV operators might be considered as Data Controllers and the use of CCTV might be deemed as processing. Using CCTV for security reasons or employee monitoring may be deemed as one of the conditions for processing of personal data without the explicit consent of the data subject, which is mandatory for the legitimate interests of the controller provided that this processing shall not violate the fundamental rights and freedoms of the data subjects. However, CCTV operators, namely controllers, still have the obligation to inform data subjects regarding the use of CCTV. This obligation may be performed through a high-visibility sign and/or public notice.

**13.2 Are there limits on the purposes for which CCTV data may be used?**

As mentioned in the answer to the previous question, there is no specific provision in the Turkish data protection legislation regarding the use of CCTV and its data. However, as per general provisions of the data protection legislation, the processing of CCTV data should be lawful, in conformity with the rules of *bona fides*, relevant with, limited to and proportionate to the purposes for which they are processed and for specific, explicit and legitimate purposes.

## 14 Employee Monitoring

**14.1 What types of employee monitoring are permitted (if any), and in what circumstances?**

There are no Turkish laws and regulations for employee monitoring. Furthermore, until the enactment of KVKK, Turkey did not have a specific law which regulates the protection and privacy of personal data. Therefore, court decisions were filling the loophole. Pursuant to court decisions, employee monitoring is permitted to the extent that it does not violate the fundamental rights and freedoms of employees.

**14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.**

Pursuant to the obligation of controllers to inform data subjects set forth by KVKK, employers must provide notice before monitoring. This may be done through adding relevant clauses to the employment agreements, specifying terms and conditions of use before handing

over company phones and computers to employees. For the use of CCTV, obligation to inform may be performed via high-visibility signs as we have previously mentioned in question 13.1.

**14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?**

This is not applicable in Turkey.

## 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.)?**

As per KVKK, the controllers are obliged to take all necessary technical and administrative measures to provide a sufficient level of security in order to prevent unlawful processing of personal data and unlawful access to personal data and to ensure the retention of personal data. In case of the processing of personal data by a natural or legal person on behalf of the controller, the controller shall jointly be responsible with these persons, namely processors, for taking the measures. The controller shall be obliged to conduct necessary inspections, or have them conducted in his own institution or organisation, with the aim of implementing the provisions of KVKK. The controllers and processors shall not disclose the personal data that they have learned to anyone in breach of KVKK, neither shall they use such data for purposes other than processing. This obligation shall continue even after the end of their term.

**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) expects voluntary breach reporting.**

In case of a breach the controller shall notify the data subject and the Board within the shortest time. Where necessary, the Board may announce such breach at its official website or through other methods it deems appropriate.

**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) expects voluntary breach reporting.**

Please see our answer to question 15.2 above.

**15.4 What are the maximum penalties for data security breaches?**

As stated below in the administrative sanctions section, the administrative fine for failing to comply with the obligations related to data security ranging from TL 15,000 to TL 1,000,000.



## 16 Enforcement and Sanctions

### 16.1 Describe the enforcement powers of the data protection authority(ies).

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
The Board shall make the necessary examination in the matters falling within its scope of work upon complaint or <i>ex officio</i> where it learnt about the alleged violation.	Those who fail to comply with the obligation to inform shall be required to pay an administrative fine of TL 5,000 to TL 100,000.	Articles of Turkish Penal Code numbered 5237 shall apply in terms of the crimes concerning personal data. The data subject may file a criminal complaint or the Board may refer a case to the public prosecutor and criminal sanctions including imprisonment may be imposed.
	Those who fail to comply with the obligations related to data security shall be required to pay an administrative fine of TL 15,000 to TL 1,000,000.	
	Those who fail to comply with the decisions issued by the Board shall be required to pay an administrative fine of TL 25,000 to TL 1,000,000.	
	Those who fail to meet the obligations for enrolling in the Registry and making a notification shall be required to pay an administrative fine of TL 20,000 to TL 1,000,000.	
	Should these acts be committed within public institutions and organisations as well as professional associations having the status of a public institution, disciplinary procedures shall be applied to the civil servants and other public officers employed in the relevant public institutions and organisations and those employed in the professional associations having the status of a public institution upon a notice by the Board and the result is communicated to the Board.	

### 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 may issue a ban on a particular processing activity and impose administrative fines and also refer the case to the public prosecutor so that criminal sanctions may be imposed, if necessary.

### 16.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

The Authority is currently exercising those powers via its resolutions. For example, new precautionary measures were recently taken by the Authority by a resolution dated 21 December 2017 and numbered 2017/61, against websites and applications collecting and sharing personal data over websites and social media, allowing users to reach phone number information upon name queries and reach name information upon phone number queries. In the said resolution, it was indicated that such activity was required to be immediately halted and applications to authorised institutions would be conducted

to prevent access to such websites and applications. Also, the resolution states that criminal complaints would be filed to the public prosecutors' offices and measures would be taken in accordance with KVKK against those who do not comply with the resolution.

### 16.4 Does the data protection authority ever exercise its powers against companies established in other jurisdictions? If so, how is this enforced?

The Authority has not yet exercised its enforcement powers against companies established in other jurisdictions.

## 17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

### 17.1 How do companies typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Requests from foreign law enforcement agencies shall be treated in line with the mutual judicial assistance treaties. Furthermore, in cases where the interest of Turkey or the data subject will seriously be harmed, personal data, without prejudice to the provisions of international agreements, may only be transferred abroad upon the permission to be given by the Board after receiving the opinions of related public institutions and organisations.

### 17.2 What guidance has/have the data protection authority(ies) issued?

The Authority currently has not issued any 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.

The Authority and the Board are now starting to function as stated in the relevant legislation. The very first indications of the Board's approach to the implementation of KVKK can be seen from the minutes of the parliament's planning and budget commission meeting dated **1 November 2017**. The Board chair Prof. Faruk Bilir stated "*In the year 2017, a total of 41 applications have been received which consist of 34 complaints and 7 denunciations. 19 of them have been finalised and a total sum of TL 125.000,00 has been imposed as an administrative fine. These applications within the year 2017 are covering all segments of society including all sectors especially media, public and banking along with electronic, insurance, informatics, telecommunication and healthcare sectors*". Please see question 16.3 for an example of a recent case.

### 18.2 What "hot topics" are currently a focus for the data protection regulator?

The hottest topic is currently the VERBİS, as the Authority announced on its website that registration obligation for controllers will begin right after the VERBİS is put into service and a beginning date is determined by the Board.

**Elvan Sevi Firat**

Firat İzgi Attorney Partnership  
Balmumcu Mahallesi  
İttri Sokak, No. 36  
34349, Beşiktaş/İstanbul  
Turkey

Tel: +90 533 242 26 56  
Email: [sevi.firat@firatizgi.com](mailto:sevi.firat@firatizgi.com)  
URL: [www.firatizgi.com](http://www.firatizgi.com)

Elvan is one of the two founding partners of the firm and she regularly supports multinational companies including manufacturers of pharmaceuticals, biotechnology, medical devices, special food and feed, cosmetics and other consumer products on important new legislative projects and policy developments in Turkey. She also advises and provides consultancy on strategic planning of new investments and start-ups in Turkey, regulatory compliance, anti-corruption and anti-trust. She also has broad litigation experience of product liability, advertising, customs controls and promotional activities. Elvan is also experienced in complex deals including: technology transfer agreements; product portfolio transfers; distribution; manufacturing; and M&As.

Elvan was deeply involved in the first-ever initiated court actions in Turkey in order to protect patent rights, including administrative court actions, as well as regulatory works before the Ministry of Health regarding enforcement of pharmaceutical patent rights, data protection and data exclusivity. She has deep-rooted experience in the data protection and privacy field coming from her 16+ years of pharma industry experience. She regularly consults multinational companies in relation to all kinds of legal matters relevant to direct selling systems and the regulatory environment. In addition to her experience in regulatory and compliance matters, Elvan regularly represents clients before the Turkish civil, criminal and administrative courts. Elvan is the author of numerous articles on regulatory issues, anti-trust and administrative law in the international trade and business media; she is a regular speaker at local and international conferences.

**Doğukan Doru Alkan**

Firat İzgi Attorney Partnership  
Balmumcu Mahallesi  
İttri Sokak, No. 36  
34349, Beşiktaş/İstanbul  
Turkey

Tel: +90 539 667 48 98  
Email: [dogukan.alkan@firatizgi.com](mailto:dogukan.alkan@firatizgi.com)  
URL: [www.firatizgi.com](http://www.firatizgi.com)

Doğukan is an associate in the Data Protection Team of the firm and his practice mainly focuses on data protection and regulatory law. Doğukan regularly advises local and multinational clients on his core specialism of data protection. In addition, pursuing an LL.M. degree in Energy Law gives him significant knowledge in energy and anti-trust law.

Doğukan has considerable experience in conducting data protection compliance projects and preparing in-company trainings for international clients. He is known for his ability to combine his social science background, coming from his major in political science, with a law perspective, which gave him the ability of thinking in an interdisciplinary way. He provides both local and international clients with legal counselling on regulatory matters.

# Firat İzgi

AVUKATLIK ORTAKLIĞI ATTORNEY PARTNERSHIP

Firat İzgi Attorney Partnership, founded by Elvan Sevi Firat and Mehmet Feridun İzgi in 2013, is a full-service law firm based in Istanbul, Turkey. Focusing on three main industries consisting of life sciences, energy and direct selling industries along with nine practice areas consisting of competition and regulatory, investigations and compliance, corporate and M&A, employment and labour litigation, dispute resolution, intellectual property, data protection and privacy, environment and climate change, and real estate and construction practices, Firat İzgi provides legal counselling and litigation services by offering carefully designed and practical legal solutions to even the most complex matters.

The firm is committed to strengthening its clients' commercial and ethical capabilities by blending legal expertise with a strong understanding of sector dynamics and commercial derivatives. Responsiveness and a proactive approach are among its strengths. The target of the firm is to be successful as a team by being a strong contributor to its clients' commercial success with high integrity. The firm's intention is to establish long-term relations with its clients and grow with them. Firat İzgi has doubled in size every year since its establishment.

# United Arab Emirates

BSA Ahmad Bin Hezeem & Associates LLP

Rima Mrad



Nadim Bardawil



## 1 Relevant Legislation and Competent Authorities

### 1.1 What is the principal data protection legislation?

The laws in the United Arab Emirates can be divided into mainland/onshore UAE laws and free-zone specific laws. The mainland of the UAE does not have any principal data protection legislation existing in its own right. Data privacy and protection is addressed across a number of separate regulations, not specifically focused on data protection.

Certain free-zones have their own respective data protection legislation which only applies within the confines of said free-zone, such as the Dubai International Financial Center (“**DIFC**”), the Abu Dhabi Global Market (“**ADGM**”), the Dubai Healthcare City (“**DHCC**”) and the mainland of the United Arab Emirates (“**UAE**”).

The principal data protection regulations in the DIFC are:

- DIFC Law Number 1 of 2007 (as amended by DIFC Law Number 5 of 2012).
- DIFC Data Protection Regulations (consolidated version number 2 of 2012) (“**DIFC Regulations**”).

The principal data protection regulations in the ADGM are:

- The Data Protection (Amendment) Regulations 2018 (“**ADGM 2018 Data Protection Regulations**”).
- The Data Protection Regulations of 2015 (“**ADGM 2015 Data Protection Regulations**” or “**ADGM Regulations**”) (enacted under Article 6(1) of Law Number 4 of 2013 concerning the Abu Dhabi Global Market) which are consistent with the Organisation for Economic Co-operation and Development’s guidelines and the European Union’s Directives on the protection of privacy and personal data.

The principal data protection legislation in the DHCC is the Health Data Protection Regulation Number 7 of 2013. It contains several detailed provisions relating to the protection of patient data and patient health information, including information about the patient’s health, medical history, disabilities, and donations of body parts and bodily substances.

The only legislation in the UAE that directly addresses Data Protection is the Dubai Law Number 26 of 2015 regulating Data Dissemination and Exchange in the Emirate of Dubai (“**the Dubai Data Dissemination Law**”). However, the Dubai Data Dissemination Law only applies to Federal Government Entities that have any data relating to Dubai, to local government entities, and to persons who produce or spread any data relating to Dubai.

### 1.2 Is there any other general legislation that impacts data protection?

The following pieces of legislation impact data protection matters in the UAE:

- Article 378 of Federal Law Number 3 of 1987 (the “**Penal Code**”), as amended by Federal Law Number 34 of 2005, provides that the violation of private or familial life by recording or transmitting private conversations and by capturing or transmitting the picture of a person in a private place is punishable by a fine and imprisonment. Article 379 of the Penal Code further provides that any individual who, by reason of his profession or situation, is entrusted with a secret and who discloses it in unauthorised cases, or uses it for his own advantage, is punishable by a fine and by imprisonment.
- Article 31 of the UAE constitution of 1971 (the “**UAE Constitution**”) provides for a general right to privacy with respect to correspondence and other means of communication: “Freedom of corresponding through the post, telegraph or other means of communication and the secrecy thereof shall be guaranteed in accordance with the law”. However, this only applies to UAE nationals.

### 1.3 Is there any sector-specific legislation that impacts data protection?

The following pieces of sector-specific legislation impact data protection matters in the UAE:

- Federal Law Number 5 of 2012 on Combatting Cybercrimes (the “**Cybercrime Law**”). Article 2 of the Cybercrime Law prohibits the disclosure, publication and re-publishing of any information that was obtained by unauthorised access to websites or electronic information systems or networks. Article 21 prohibits the use of a computer network, an electronic information system or any information technology means for the invasion of privacy. Further, Article 22 states that any person who uses, without permission, any information network, electronic site or information technology tool to expose confidential information shall be punished by imprisonment and a fine.
- Federal Law by Decree Number 3 of 2003 regarding the Organisation of the Telecommunications Sector (the “**Telecommunications Law**”). The Telecommunications Law provides protection to all data obtained through any means of communication. In addition, the 2014 Customer Protection Regulations address to what extent the UAE’s two telecommunication companies can share the personal details of their customers.
- Telecommunications Regulatory Authority Consumer Protection Regulations Version 1.3 protect data and

information relating to telecommunications subscribers, including their name, address, bank account details, credit card details, and message and call recordings.

- Dubai Law Number 23 of 2006 (the “**Dubai Statistics Law**”) prevents the disclosure of any data collected for statistics.
- Federal Law Number 15 of 1980 regarding Printed Matters and Publications provides that publishing news and comments connected with a person’s private life is prohibited.
- UAE Cabinet Resolution No. 21 of 2013 addressing data security for Federal Authorities (the “**Data Security Resolution**”) specifically outlines how data belonging to the UAE federal government, authorities, ministries and other official entities must be stored, treated and disseminated.

In the healthcare settings, privacy and data protection matters are governed by the regulations listed below. Emirate-specific regulatory bodies have begun drafting more comprehensive medical data legislation.

- Health Authority of Abu Dhabi (“**HAAD**”) Data Standards and Procedures, of January 2008, as revised by the April 2014 version. The HAAD Data Standards and Procedures outlines the policies and procedures which must be followed when handling Confidential Health Information (“**CHI**”) focusing on four areas: the necessary and authorised access to CHI; the unauthorised access to CHI; the storage of CHI; and the transmission of CHI. It further provides regulations relating to health insurance fraud. The HAAD has created a Data Standards Panel whose role is to “review and recommend to HAAD changes and additions to electronic data exchange standards, such as transactions, codes and business rules”.
- Dubai Health Authority (“**DHA**”) Home Healthcare Regulations, issued in 2012, outline the procedures healthcare facilities must follow with respect to healthcare records and their management. Similarly, the Health Record Guidelines outline the essential requirements which healthcare facilities must implement with regards to the management of health records including record keeping, retention of health records and destruction of health records. The DHA also created the Health Data and Information Analysis Department whose role is to improve the manner and method in which health data is handled and exchanged, as well as to “focus on transparency and confidentiality” between patients and healthcare providers.
- Federal Law Number 7 of 1975 concerning the Practice of the Human Medicine Profession (the “**Human Medicine Profession Law**”). Article 13 of the Human Medicine Profession Law states that a doctor has no right to divulge a private secret concerning a patient and relating to his profession. Certain exceptions apply to this, namely if divulging the secret is held to serve the interests of the individual or to prevent a crime from occurring.
- The Ministry of Health Code of Conduct 1988 (the “**Code of Conduct**”) states that pharmacists are required to uphold the confidentiality of any information acquired in the course of professional practice relating to patients and their families. In this case, confidential information and data extends beyond the customer’s medical details and includes their address, telephone, and any family or financial data contained in the medical record and hospital registration details.
- Other guidelines on the ethical principles to respect in relation to confidentiality and privacy are covered by “the Good Clinical Practice Principles” and “the Basic Principle for all Medical Research”.

#### 1.4 What authority(ies) are responsible for data protection?

There is no single authority responsible for the regulation of data protection in the United Arab Emirates. The following sector-

specific authorities are responsible for matters related to data protection in the United Arab Emirates:

- National Electronic Security Authority (pursuant to the Cybercrime Law).
- Telecommunications Regulatory Authority (pursuant to the Telecommunications Law).
- The Dubai Statistics Centre (pursuant to the Dubai Statistics Law).
- The Dubai Health Authority and the Health Authority of Abu Dhabi.

In the DIFC, the Office of the Data Protection Commissioner is responsible for the regulation of data protection.

In the ADGM, the Office of Data Protection is responsible for regulating data protection matters.

In the DHCC, the Centre for Healthcare Planning and Quality is responsible for the regulation of data protection.

## 2 Definitions

### 2.1 Please provide the key definitions used in the relevant legislation:

- **“Personal Data”**  
The DIFC Law Number 1 of 2007 defines “Personal Data” as any data referring to an identifiable natural person, which in turn is defined as a natural living person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to their biological, physical, biometric, physiological, mental, economic, cultural or social identity.  
The ADGM 2018 Data Protection Regulations define “Personal Data” as any information relating to an identified natural person or identifiable natural person. “Identifiable natural person” is defined as a natural person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to their biological, physical, biometric, physiological, mental, economic, cultural or social identity.
- **“Processing”**  
In the DIFC Law Number 1 of 2007, “Processing” is defined as any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.  
The ADGM 2018 Data Protection Regulations define “Processing” as any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction, and “Processed”, “Processes” and “Process” shall be construed accordingly.
- **“Controller”**  
In the DIFC Law Number 1 of 2007 and the ADGM 2018 Data Protection Regulations, “Data Controller” is defined as any person in the DIFC or the ADGM, respectively, who alone or jointly with others determines the purposes and means of the processing of personal data. A data controller is equivalent to a data protection officer.
- **“Processor”**  
In the DIFC Law Number 1 of 2007 and the ADGM 2018



Data Protection Regulations, a “Data Processor” is any person who processes personal data on behalf of a data controller.

#### ■ **“Data Subject”**

In the DIFC Law Number 1 of 2007, “Data Subject” is defined as any individual to whom personal data relates. The ADGM 2018 Data Protection Regulations define “Data Subject” as the natural person to whom personal data relate.

#### ■ **“Sensitive Personal Data”**

In the DIFC Law Number 1 of 2007, “Sensitive Personal Data” is defined as personal data revealing or concerning (directly or indirectly) racial or ethnic origin, communal origin, political affiliations or opinions, religious or philosophical beliefs, criminal record, trade-union membership and health or sex life. The ADGM 2018 Data Protection Regulations provides the same definition of “Sensitive Personal Data” although it does include communal origin in the definition.

#### ■ **“Data Breach”**

None of the applicable laws provide a definition of “Data Breach”.

#### ■ **Other key definitions – please specify (e.g., “Pseudonymous Data”, “Direct Personal Data”, “Indirect Personal Data”)**

##### ■ **“Data”**

In the DIFC Law Number 1 of 2007 and the ADGM 2018 Data Protection Regulations, “Data” is defined as any information which:

- (a) is processed by means of equipment operating automatically in response to instructions given for that purpose;
- (b) is recorded with the intention that it should be processed by means of such equipment; or
- (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system.

In the Dubai Data Dissemination Law, “Data” is defined as a collection of organised or unorganised information, facts, concepts, instructions, observations, or measurements, in the form of numbers, alphabets, symbols, images, or any other form, that are collected, produced or processed by data providers. “Data” also includes 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 UAE’s data protection laws only apply to businesses established in the mainland of the UAE and to businesses established in free-zones which are not governed by any specific data protection laws. Free-zones that have issued their own data protection legislation, such as the DIFC and the ADGM, are not governed by the laws of the United Arab Emirates that relate to data protection.

### 4 Key Principles

#### 4.1 What are the key principles that apply to the processing of personal data?

##### ■ **Transparency**

Although there is no explicit reference to having a right to transparency in the mainland of the UAE, an individual’s right

to a private life may mean that they have a right to transparency, or a right to know how their personal data is being used.

In the DIFC and the ADGM, the rights to access to and rectification, erasure or blocking of personal data and the rights to object to processing provided by Articles 17-18 of the DIFC Law Number 1 of 2007 and Articles 10-11 of the ADGM 2015 Data Protection Regulations give individuals located in these jurisdictions a right to transparency.

##### ■ **Lawful basis for processing**

In the mainland of the UAE, the DIFC and the ADGM, there must be a lawful basis for processing data. The DIFC and the ADGM have set out similar circumstances in which sensitive personal data can be processed. Article 10(1) of the DIFC Law Number 1 of 2007 and Article 3 of the ADGM 2015 Data Protection Regulations both state that sensitive personal data shall only be processed in the following circumstances: (a) if the data subject has given his written consent to the processing of the sensitive personal data; (b) if the processing is necessary for the purposes of carrying out the obligations and specific rights of the data controller; (c) if the processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; (d) if the processing is carried out in the course of its legitimate activities with appropriate guarantees by any non-profit seeking body, provided that the personal data is not disclosed to a third party without the consent of the data subject; (e) if the processing relates to personal data which are manifestly made public by the data subject or which is necessary for the establishment, exercise or defence of legal claims; (f) if the processing is necessary for compliance with any regulatory or legal obligation to which the data controller is subject; (g) if the processing is necessary to uphold the legitimate interests of the data controller recognised in the international financial markets; (h) if the processing is necessary to comply with any regulatory requirements; and (i) if the processing is required for medical reasons.

In the DIFC, sensitive personal data can also be processed in the following circumstances: (j) if the processing is required for protecting members of the public against: (i) financial loss due to dishonesty, malpractice or other seriously improper conduct by persons concerned in the provision of certain business activities; and (ii) dishonesty, malpractice or other seriously improper conduct by persons concerned in the provision of certain business activities.

If a business wishes to process data in any circumstances other than those mentioned above in the DIFC and the ADGM, Article 10(2)(a) of the DIFC Law Number 1 of 2007 and Article 3(2) of the ADGM 2015 Data Protection Regulations state that they should obtain a permit to process this sensitive personal data.

##### ■ **Purpose limitation**

Please see “Data minimisation” below.

##### ■ **Data minimisation**

In the mainland of the UAE, an individual’s right to privacy is protected. If, however, this individual consents to their personal information being used for a specific purpose, the information should not be used for a purpose that goes beyond the purpose agreed on.

In the DIFC and the ADGM, given that an individual’s consent must be obtained to be able to process their personal data, the data collected and processed should not be used for any purpose beyond the purpose agreed on.

In all jurisdictions, information should be used in a manner proportionate to what it was initially collected for.

##### ■ **Proportionality**

Please see “Data minimisation” above.



## ■ Retention

In the mainland of the UAE, there are no specifications as to how long personal data can be retained.

In the DIFC and the ADGM, Article 8 of the DIFC Law Number 1 of 2007 and Article 1 of the ADGM 2015 Data Protection Regulations provide that personal data should not be kept for longer than is necessary for the purposes for which the personal data was collected or for which they are further processed.

In the ADGM, Article 51 of the ADGM Employment Regulations on processing personal data by the employer also provides that personal data must not be kept for longer than is necessary by the employer (having regard to the purpose or purposes for which they are being processed).

## ■ Other key principles – please specify

There are no other key principles to be aware of.

## 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

There is no such right for individuals in the mainland of the UAE.

Article 17 of the DIFC Law Number 1 of 2007 and Article 10 of the ADGM 2015 Data Protection Regulations each respectively give data subjects in the DIFC, and in the ADGM, the right to access and to rectify, erase or block personal data. This must be done at reasonable intervals and without excessive delay or expense. This includes the right to delete information.

#### ■ Right to rectification of errors

Please see “Right of access to data/copies of data” above.

#### ■ Right to deletion/right to be forgotten

Please see “Right of access to data/copies of data” above.

#### ■ Right to object to processing

In the mainland of the UAE, an individual’s privacy is protected by the UAE Constitution, the UAE Penal Code and the UAE Cybercrime Law. This gives individuals an implied right to object to the processing of their personal data, to restrict its processing, and to object to its marketing.

Article 18 of the DIFC Law Number 1 of 2007 and Article 11 of the ADGM 2015 Data Protection Regulations each give data subjects in the DIFC, and in the ADGM, the right to object to processing on reasonable grounds at any time. Given that the objection can be done at any time, this implies that data subjects in the DIFC and the ADGM also have a right to restrict processing and to withdraw consent. A data subject has the right to be informed before personal data is disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object to such disclosures or uses. Data subjects have the right to object to marketing in the DIFC and the ADGM.

#### ■ Right to restrict processing

Please see “Right to object to processing” above.

#### ■ Right to data portability

No explicit references are made to the right to data portability under UAE, DIFC and ADGM regulations.

#### ■ Right to withdraw consent

Please see “Right to object to processing” above.

## ■ Right to object to marketing

Please see “Right to object to processing” above.

## ■ Right to complain to the relevant data protection authority(ies)

In the mainland of the UAE, an individual’s privacy is protected by the UAE Constitution, the UAE Penal Code and the UAE Cybercrime Law. This gives individuals an implied right to complain to the relevant authority.

In the DIFC, according to Article 7(1)(1) of the DIFC Data Protection Regulations, a person has a right to complain. A person may file a claim with the commissioner of data protection by lodging a written notice that provides the following information:

- (a) full name and address of the person making the claim;
- (b) the data controller whom the person believes has contravened the law;
- (c) a detailed statement of facts which the person believes gives rise to contravention of the law; and
- (d) the relief sought by the person making the claim.

In the ADGM, under Article 18 of the ADGM 2015 Data Protection Regulations, a person has a right to complain to the Registrar in respect of the processing of their personal data.

## ■ Other key rights – please specify

There are no other key rights to be aware of.

## 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 the United Arab Emirates, there are no legal obligations on businesses to register with or notify any authority that manages data protection matters in respect of data processing activities. Data can be processed as long as data relating to an individual was obtained with their consent or if it is required by law. Further, there is no specific data protection authority in the United Arab Emirates. The lone exception here relates to data belonging to the UAE government. The Data Security Resolution outlines that consent must be provided before any data owned by the UAE government can be stored, transferred or shared.

The DIFC has seen the implementation of a more regulated system of data protection. Companies operating in the DIFC must appoint a data controller. Article 19 of the DIFC Law Number 1 of 2007 and Article 6 of the DIFC Data Protection Regulations state that the data controller of a business which is processing personal data must file a notification with the commissioner of data protection. The data controller should establish and maintain records of any personal data processing operations. It should be noted that even where a data controller does not process personal data, it must still submit a notification reflecting this.

Similarly, companies operating in the ADGM must appoint a data controller. Article 12 of the ADGM Data Protection Regulations of 2015 provides that to be entitled to operate as a data controller, an individual must first be registered as a data controller with the ADGM Registrar.

---

**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)?**

---

In the DIFC, according to clause 6(3)(2) of the DIFC Data Protection Regulations, when a data controller gives a notification to the commissioner of data protection, it must be specific. The notification must contain the following information:

- (a) a general description of the personal data Processing being carried out;
- (b) an explanation of the purpose for the personal data processing;
- (c) the data subjects or class of data subjects whose personal data is being processed;
- (d) a description of the class of personal data being processed; and
- (e) a statement of the jurisdictions to which personal data will be transferred by the data controller, along with an indication as to whether the particular jurisdiction has been assessed as having an adequate level of protection in accordance with the terms of the DIFC Law Number 1 of 2007.

Details of the person responsible for data protection compliance must also be provided.

The ADGM Data Protection Regulations do not set any specific requirements for the registration of a data controller with the Registrar. Article 12 of the ADGM 2015 Data Protection Regulations states that a data controller must notify the Registrar of its intention to become a data controller in the required form. They should also establish and maintain records of any personal data processing operations or any set of such operations.

---

**6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?**

---

According to Article 19(2) of the DIFC Law Number 1 of 2007, in the DIFC, notifications are made based on data categories. Clause 6(3)(1) of the DIFC Data Protection Regulations provides that a data controller must notify the commissioner of data protection in the following circumstances:

- (a) for any personal data processing operation or set of operations involving the processing of sensitive personal data; and
- (b) for any personal data processing operation or set of operations involving the transfer of personal data to a recipient outside of the DIFC which is not subject to laws and regulations which ensure an adequate level of protection.

Further, if the manner of processing is changed, the data controller must submit a notification to the commissioner of data protection informing them of this.

Even where a data controller does not process personal data, it must still submit a notification reflecting this.

In the ADGM, notifications are also made based on data 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)?**

---

In the mainland of the UAE, there is no requirement to register with or notify any data protection authority as there is no such data protection authority.

Entities operating in the DIFC and the ADGM must register with the relevant data protection authority in the DIFC and the ADGM, respectively.

According to Article 19 of the DIFC Law Number 1 of 2007, in the DIFC, the appointed data controller is responsible for filing the notification with the relevant data protection authority.

According to Article 12 of the ADGM 2015 Data Protection Regulations, the data controller must register themselves with the relevant 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)?**

---

For the information that must be included in a notification, please see question 6.2.

---

**6.6 What are the sanctions for failure to register/notify where required?**

---

As stated previously, there is no requirement to register/notify in the mainland of the UAE.

In the DIFC, failure to register with the Office of the Commissioner of Data Protection will result in a fine of \$25,000.

The ADGM regulations do not set out any sanctions for failure to register, although they should be levied in this event.

---

**6.7 What is the fee per registration/notification (if applicable)?**

---

According to the DIFC Data Protection Regulations, the fee for the notification is \$1,000 for entities regulated by the Dubai Financial Services Authority (the regulating authority of the Dubai International Financial Center), \$500 for Dubai Financial Services Authority non-regulated entities except for retail, and \$200 for retail entities. A notification filed by a data controller who does not process any personal data does not require a fee.

According to ADGM 2015 Data Protection Regulations, the fee for the application for the initial registration as a data controller is \$300.

---

**6.8 How frequently must registrations/notifications be renewed (if applicable)?**

---

In the DIFC, the notification validity period is one year. Failure to renew the notification constitutes a breach of the DIFC Law Number 1 of 2007.

In the ADGM, according to Article 12(4) of the ADGM 2015 Data Protection Regulations (as amended by the 2018 Regulations) registration notifications must be submitted to the Registrar on annual basis where the personal data processing is to continue in the subsequent year.

---

**6.9 Is any prior approval required from the data protection regulator?**

---

In the DIFC, there is no prior approval required from the data protection regulator. In the ADGM, approval to work as a data controller will be granted after the registration notification has been submitted.

**6.10 Can the registration/notification be completed online?**

In the DIFC, the notification must be completed online; it is available on the Client Portal. In the ADGM, the registration can also be completed online.

**6.11 Is there a publicly available list of completed registrations/notifications?**

Both in the DIFC and the ADGM, there is no publicly available list of completed notifications.

**6.12 How long does a typical registration/notification process take?**

No specific period of time is provided as to how long a typical notification process takes in the DIFC and ADGM regulations.

**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 in the mainland of the United Arab Emirates. In contrast, in the DIFC and the ADGM, the appointment of a Data Protection Officer is mandatory. Certain requirements are imposed on data controllers in these free-zones. As per Article 8 of the DIFC Law Number 1 of 2007 and Article 1 of the ADGM 2015 Data Protection Regulations, data controllers should ensure that the personal data which they process is processed securely, and for specified and legitimate purposes.

**7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?**

In the DIFC and the ADGM, failure to appoint a Data Protection Officer will result in a fine.

**7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect to his or her role as a Data Protection Officer?**

The DIFC and ADGM data protection regulations do not provide any such protection to the data protection officer.

**7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?**

The DIFC and ADGM regulations do not provide any guidance on whether a single data protection officer can cover multiple entities.

**7.5 Please describe any specific qualifications for the Data Protection Officer required by law.**

The DIFC and ADGM regulations do not set out any specific qualifications that data controllers are required to have.

**7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?**

Article 8(1) of the DIFC Law Number 1 of 2007 and Article 1 of ADGM 2015 Data Protection Regulations require data controllers to ensure that the personal data which they process be:

- (a) processed fairly, lawfully and securely;
- (b) processed for specified, explicit and legitimate purposes in accordance with the data subject's rights and that it is not processed in a way incompatible with those purposes or rights;
- (c) adequate, relevant and not excessive in relation to the purposes for which it is collected and/or further processed;
- (d) accurate and, where necessary, kept up to date; and
- (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data was collected or for which they are further processed.

Moreover, in the DIFC, according to Article 8(2) of the DIFC Law Number 1 of 2007, every reasonable step must be taken by the data controller to ensure that personal data which is inaccurate or incomplete, having regard to the purposes for which it was collected or for which it is further processed, is erased or rectified. According to Article 16(1) of the DIFC Law Number 1 of 2007, the data controller should also implement appropriate technical and organisational measures to protect personal data against willful, negligent, accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure of access and against all other unlawful forms of processing.

In this vein, Article 9 of the ADGM 2015 Data Protection Regulations provides that the data controller must implement appropriate technical and organisational measures to protect Personal Data in the ADGM.

**7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?**

In the DIFC, the appointment of a data protection officer must be registered. The commissioner maintains a public register of data controllers. Each register entry includes the name and address of the data controller, and a general description of their processing of personal data.

According to Article 12 of the ADGM 2015 Data Protection Regulations, the appointment of a data protection officer must be registered with the ADGM Registrar.

**7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?**

In the DIFC, the data controller must be named in a public register maintained by the commissioner. Individuals can consult the public register to find out details of the processing of personal data being carried out by a specific data controller.

Similarly, in the ADGM, data controllers are listed in the data controller register. The data controller register is incorporated within the ADGM Public Register of Companies.

## 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?

Although it is not explicitly set out in the DIFC and ADGM regulations, it is advisable for a business wishing to appoint a processor to process personal data on its behalf to enter into a service agreement with that 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.)?

It is advisable to have a signed and stamped agreement written on letterhead, that addresses the data controller's responsibilities with respect to the procedure for processing personal data, keeping this data secure, only processing it in accordance with instructions and in accordance with the provisions of a specific law.

## 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 2009, the Telecommunications Regulation Authority issued its 'Regulation on Unsolicited Electronic Communication' addressing electronic direct marketing, including spam emails, spam text messages and telephone calls. The Regulation on Unsolicited Electronic Communication confirms that mobile phone marketing providers must obtain consent from customers before they send them marketing messages, before they email them or even before they call them. The issue is that people will have generally unknowingly consented to their information being used for marketing purposes. In support of this, Article 72 of the UAE Telecommunications Law penalises copying or disclosing the content of any sort of communication without having the right to do so.

It is worth noting that Article 31 of the UAE Constitution states that an individual has the right to enjoy freedom of communication by post, telegraph or other means of communication and the secrecy thereof is to be guaranteed in accordance with the law.

The UAE Cybercrime Law sets out harsh penalties for using an individual's personal information without their consent or that is otherwise unauthorised by law. Article 21 of the UAE Cybercrime Law states that whoever uses a computer network, an electronic information system or any information technology means for the invasion of privacy of another person shall be sanctioned.

Further, Article 17.22 of the Consumer Protection Regulations, issued on 10 January 2017, provides that advertising (which is defined to include electronic direct marketing) must not be unduly intrusive or coercive and shall not harass or be likely to harass customers. If the marketing method in question is judged to be unduly intrusive or harassing, restrictions will be imposed on this marketing method.

In the DIFC and the ADGM, personal data may only be processed in certain conditions, according to Article 9 of the DIFC Law Number 1 of 2007 and article 2 of the ADGM 2015 Data Protection Regulations. The principal condition is obtaining the data subject's written consent for the processing. Restrictions will be imposed on electronic direct marketing conducted without the individual's consent.

In addition, according to Article 13 of the DIFC Law Number 1 of 2007 and Article 7 of the ADGM 2015 Data Protection Regulations, where information about a data subject has been obtained, the data subject will need to be informed of whether their information will be used for direct marketing purposes, in so far as such information is necessary to guarantee fair processing in respect of the data subject.

### 9.2 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 question 11.1.

### 9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

The restrictions noted above are aimed at protecting an individual's right to consent to their personal information being used. Although the laws and regulations referred to above will protect this right for an individual living in the UAE, the UAE Government does not have the authority to impose any sanctions on marketing sent from other jurisdictions.

### 9.4 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

The Telecommunications Regulation Authority (mainland UAE jurisdiction), the Office of the Data Protection Commissioner (DIFC jurisdiction) and the Office of Data Protection (ADGM jurisdiction) are active in the enforcement of breaches of marketing restrictions.

### 9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

To be able to purchase marketing lists from third parties, the information of the business/individual on the list must have been obtained with their consent and the individual must have also consented to their information being used by a third party.

### 9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

Article 21 of the UAE Cybercrime Law states that whoever uses a computer network, an electronic information system or any information technology means for the invasion of privacy of another person shall be punished by imprisonment of a period of at least six months, and a fine not in excess of five hundred thousand dirhams, or either of these two penalties.



## 10 Cookies

### 10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

In the mainland jurisdiction of the UAE, there are no specific legislative restrictions relating to the use of cookies. Despite this, the UAE Cybercrime Law can be construed to apply to cookies. Given that Article 21 of the UAE Cybercrime Law prohibits the use of a computer network for the invasion of privacy, the storage of information by a cookie can be held as an invasion of privacy, and therefore a breach of the Cybercrime Law.

Although the DIFC and ADGM regulations do not set out any legislative restrictions directly concerned with cookies, they do set out restrictions with regards to the processing of personal data – which is stored by cookies. Cookies that store personal data can therefore be indirectly restricted by the DIFC Regulations.

### 10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

The applicable restrictions do not make a distinction 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 relevant data protection authorities in the mainland of the UAE, in the DIFC and in the ADGM have not taken any enforcement actions in relation to cookies.

### 10.4 What are the maximum penalties for breaches of applicable cookie restrictions?

In the mainland jurisdiction of the UAE, the maximum penalty for the breach of restrictions relevant to cookies (the breach of Article 21 of the UAE Cybercrime Law) is imprisonment of a period of at least six months and a fine not in excess of five hundred thousand dirhams, or either of these two penalties.

## 11 Restrictions on International Data Transfers

### 11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

In the mainland of the UAE, there are no restrictions on the transfer of personal data to other jurisdictions. Notwithstanding this, Article 378 of the Penal Code provides that data subjects should provide their consent to the transfer of data relating to them both inside and outside the UAE.

In the DIFC and the ADGM, according to Article 11 of the DIFC Law Number 1 of 2007 and Article 4 of the ADGM 2015 Data Protection Regulations, a transfer of personal data to a recipient located in a jurisdiction outside the DIFC and the ADGM may take place only if an adequate level of protection for that personal data is ensured by regulations that are applicable to the recipient (if the jurisdiction is listed as an acceptable jurisdiction under the regulations). Transfers

of personal data to a recipient which is not subject to regulations and which ensure an adequate level of protection may take place if certain conditions are met, according to Article 12 of the DIFC Law Number 1 of 2007 and Article 5 of the ADGM 2015 Data Protection Regulations. For instance, among other conditions, the following requirements must be met:

- the data controller has obtained a permit from the commissioner of data protection;
- the data subject has given his written consent to the proposed transfer;
- the transfer is necessary for the performance of a contract between the data subject and the data controller, or the implementation of pre-contractual measures taken in response to the data subject's request; and
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the data controller and a third party.

### 11.2 Please describe the mechanisms companies 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 the mainland of the UAE, the data subject's written consent must be obtained.

In the DIFC and the ADGM, companies will typically utilise the performance of a contract with the data subject and the performance of a contract in the interest of the data subject, among other conditions, to transfer 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.

No prior approval is required in the mainland of the UAE.

In the DIFC and the ADGM, approval is required, respectively, from the DIFC Commissioner of Data Protection and from the ADGM Registrar to be able to transfer personal data to a recipient located outside the jurisdiction; this is given to the data controller in the form of a permit.

## 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.)?

In Dubai, Article 19 of Dubai Law Number 4 of 2016 on Financial Crimes provides protection to whistle-blowers, or people who report crimes related to financial matters – in this case to the Dubai Centre for Economic Security. The law does not set out any specification on whistle-blowing in these circumstances. In contrast, with regards to non-financial crimes in Emirates other than Dubai, Article 379 of the Penal Code states that it is an offence for an individual to disclose secrets which they have been entrusted with as a result of their employment.



The DIFC regulations do not provide any guidance on the permitted scope of corporate whistle-blowing, although Article 10(1)(h) of the DIFC Law Number 1 of 2007 allows the processing of personal data if it is necessary to comply with any regulatory requirements, auditing, accounting, anti-money laundering, or counter-terrorist financing obligations or the prevention or detection of any crime that apply to a data controller.

Similarly, the ADGM Regulations do not provide any guidance on the permitted scope of corporate whistle-blowing, although Article 3(1)(h) of the ADGM 2015 Data Protection Regulations allows the processing of personal data if it is necessary to comply with any regulatory requirements, auditing, accounting, anti-money laundering, or counter-terrorist financing obligations or the prevention or detection of any crime that applies to a data controller.

### **12.2 Is anonymous reporting prohibited, or strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do companies typically address this issue?**

Anonymous reporting is not prohibited in the United Arab Emirates. On the contrary, it is encouraged. In 2011, the police launched a service called 'Najeed' which allows the public to report crimes to the police in a fully confidential manner.

## **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)?**

In the mainland of the UAE, there is no separate registration requirement for the use of CCTV (Closed Circuit Television). In accordance with Article 378 and 379 of the UAE Penal Code and the UAE Cybercrimes Law, given that a person's right to privacy is protected, this right to privacy will need to be taken into account when installing CCTV. Article 378 of the UAE Penal Code stipulates that 'a person shall be punished by detention and a fine if he prejudices the privacy of the individual or family life by committing any of the following acts other than in the events as permitted by law or without the consent of the victim: to eavesdrop, record or transmit by any device of any kind whatsoever conversations in a private place or by way of telephone or any other device, to take or transmit by any device of any kind whatsoever a photo of a person in a private place [...]'. This means that a high-visibility sign, or other forms of appropriate signage, needs to be displayed, if CCTV is installed or that prior written consent needs to be obtained from individuals who may be recorded by CCTV in a specific area.

Dubai Law Number 24 of 2008 (as amended by Law Number 10 of 2014) provides regulations on the use of CCTV in the Emirate of Dubai. Article 16 of the Dubai Law Number 24 of 2008 enumerates the business activities that must satisfy certain security specifications including employing CCTV surveillance. These include hotels and short-stay residences, financial and monetary institutions, the manufacture and sale of precious metals and stones, shooting ranges, military and hunting equipment stores, shopping and leisure centres, precious materials storage facilities, hazardous materials storage facilities, precious commodities stores/outlets, large department stores, petrol stations, internet services, storage services, aircraft and balloon clubs.

The use of CCTV does not require separate registration/notification in the DIFC and the ADGM.

### **13.2 Are there limits on the purposes for which CCTV data may be used?**

The purposes for which CCTV data may be used remains largely unregulated in the UAE. There are no specifications as to the purpose of carrying out monitoring through CCTV yet companies are usually equipped with these devices when they are necessary for the organisation and maintenance of security, depending on the type of activity carried out by the company. Nevertheless, as a general rule, recorded footage should not be used abusively by the employer and the CCTV must not be placed in private areas such as in the toilets and in the prayer rooms.

The DIFC and ADGM Regulations do not provide any 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?**

Although there are no sector-specific legislations relevant to employee monitoring in the UAE, a combination of federal, local and free-zone laws are applicable on employers and employees. These laws (such as Article 31 of the UAE Constitution which gives individuals a right to secrecy in their communications) guarantee the right to privacy and safeguarding of personal data of the employee, and may be potentially applicable on instances such as the monitoring and recording of telephone conversations in the workplace. There are no specifications on monitoring employees through the use of CCTV, although employees will have a right of privacy in this regard. As a general rule, employers have the right to monitor and access the company's property which include email servers, devices such as mobile phone, laptops and tablets.

Many businesses are required, by nature, to monitor telephone conversations as a way for managing risk such as banks, trading houses, insurance and brokerage companies. Other companies that are not required by nature to monitor telephone conversations may decide to do so for training purposes and/or to ensure the quality of the services provided by its employees.

In the DIFC, according to DIFC Law Number 1 of 2007, the employee's consent must be obtained to be able to monitor, record or process any personal data related to them (whether by telephone, by CCTV or by email).

In the ADGM, Article 51 of the ADGM Employment Regulations on processing personal data by the employer provides that personal data must not be kept 'for longer than is necessary' by the employer (having regard to the purpose or purposes for which they are being processed).

### **14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.**

In the mainland of the UAE, according to Federal Laws, specifically the Cybercrime Law, Telecommunications Law and the Penal Code, the employee's consent will have to be obtained in order to be able to monitor them. This provision can be included in the employee's employment contract or in the company's internal policies. With respect to monitoring the employee's emails, the fact that the email server belongs to the company's assets implies that the company will have full access to the server.

In the DIFC, according to DIFC Law Number 1 of 2007, the employee's consent must be obtained to be able to monitor, record or process any personal data related to them (whether by telephone, by CCTV or by email). The same requirements apply to the ADGM.

#### **14.3 To what extent do works councils/trade unions/ employee representatives need to be notified or consulted?**

There are no work councils or any such unions in the UAE.

### **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 mainland of the UAE, the protection guaranteed to an individual's right to privacy implies that there is a general obligation to ensure the security of their personal data. There is no specific authority responsible for ensuring that data are kept secure.

In the DIFC, article 16 of the DIFC Law Number 1 of 2007 imposes an obligation on the data controller to ensure the security of personal data. Article 16 provides that the data controller must implement appropriate technical and organisational measures to protect personal data.

In the ADGM, article 9 of the ADGM 2015 Data Protection Regulations provides that the data controller must ensure the security of the personal data being processed by implementing appropriate technical and organisational measures.

#### **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) expects voluntary breach reporting.**

In the mainland of the UAE, there is no such requirement given that there is no data protection authority.

In the DIFC, Article 16(4) of the DIFC Law Number 1 of 2007 provides that the data controller or the data processor must inform the commissioner of data protection in the event of an unauthorised intrusion to any personal database, whether physical, electronic or otherwise. This must be done 'as soon as practicably possible'. Failure to do so will result in a fine of \$5,000.

In the ADGM, there is no specific requirement to report data 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) expects voluntary breach reporting.**

In the mainland of the UAE, there is no such requirement given that there is no data protection authority.

In the DIFC, there is no requirement to report data breaches to affected data subjects. There is a requirement, according to Article 13 of the DIFC Law Number 1 of 2007, for the data controller to provide the data subject with the following information upon commencing to collect personal data about them:

- (a) the identity of the data controller;
- (b) the purposes of the processing for which the personal data are intended; and
- (c) other information such as the recipients or categories of recipients of the personal data, the existence of the right of access to and the right to rectify the personal data concerning them, and whether the personal data will be used for direct marketing purposes, among other conditions.

In the ADGM, there is no legal requirement to report data breaches to affected data subjects. However, according to Article 6 of the ADGM 2015 Data Protection Regulations, data controllers must provide a data subject whose personal data has been collected with the following information:

- (a) the identity of the data controller;
- (b) the purposes of the processing for which the personal data are intended; and
- (c) other information such as the recipients or categories of recipients of the personal data, the existence of the right of access to and the right to rectify the personal data concerning them, and whether the personal data will be used for direct marketing purposes, among other conditions.

#### **15.4 What are the maximum penalties for data security breaches?**

In the mainland of the UAE, the penalties for non-compliance are as follows:

- Article 15 of the UAE Cybercrimes Law states that any person who captures or intercepts any communication through any information network, intentionally and without permission, shall be punished by imprisonment and a fine not less than AED 150,000 (approx. €33,870) and not exceeding AED 500,000 (approx. €112,910) or by any of these punishments. Any person who disclosed the information obtained unlawfully by receiving or interception of communications shall be punished by imprisonment for a period not less than one year.
- Article 21 of the UAE Cybercrime Law stipulates that a person who used an information network, electronic information system or any of the information technology tools in invading the privacy of a person in cases other than those permitted in Law shall be punished by imprisonment for a period not less than six months, and a fine not less than AED 150,000 (approx. €33,870) and not exceeding AED 500,000 (approx. €112,910) or by any of these punishments by any of the following methods:
  - overhearing, interception, recording, transferring, transmitting or disclosure of conversations, communications or audio or visual materials;
  - capturing pictures of a third party or preparing electronic pictures or transferring, exposing, copying or keeping those pictures; and/or
  - publishing electronic news or pictures or photographs, scenes, comments, statements or information even if they were correct and real.
- Article 22 of the UAE Cybercrime Law states that any person who used without permission any information network, electronic site or information technology tool to expose confidential information obtained by occasion or because of

his work shall be punished by imprisonment for a period not less than six months, and a fine not less than AED 500,000 (approx. €112,910) and not exceeding AED 1,000,000 (approx. €225,815) or by any of these punishments.

In the DIFC, the following penalties apply:

- Maximum fine of \$15,000 for failing to process data in accordance with Article 8 of the DIFC Law Number 1 of 2007.
- Maximum fine of \$15,000 for failing to comply with legitimate processing requirements in accordance with Article 9 of the DIFC Law Number 1 of 2007.
- Maximum fine of \$20,000 if a data controller transfers personal data outside the DIFC in accordance with Article 12(1)(a) of the DIFC Law Number 1 of 2007 and failing to obtain a permit from the commissioner of data protection.

In the ADGM, according to Article 17(3) of the ADGM 2015 Data Protection Regulations, a data controller who fails, without reasonable excuse, to comply with any direction issued by the registrar under section 17(3) shall be liable to a fine of \$15,000.

## 16 Enforcement and Sanctions

### 16.1 Describe the enforcement powers of the data protection authority(ies).

Authority	Investigatory Power	Civil/ Administrative Sanction	Criminal Sanction
Commissioner of Data Protection (DIFC)	<ul style="list-style-type: none"> <li>■ Accessing personal data processed by data controllers or data processors</li> </ul>	<ul style="list-style-type: none"> <li>■ Issuing warnings or admonishments and making recommendations to data controllers</li> <li>■ Initiating proceedings for contraventions of the law before the Court</li> <li>■ Imposing fines in the event of non-compliance with its directions</li> <li>■ Imposing fines for non-compliance with the DIFC Law Number 1 of 2007</li> <li>■ Initiating a claim for compensation on behalf of a data subject before the court</li> <li>■ Acquiring, holding and disposing of property of any description</li> </ul>	

Authority	Investigatory Power	Civil/ Administrative Sanction	Criminal Sanction
Registrar (ADGM)	<ul style="list-style-type: none"> <li>■ Access personal data processed by data controller or data processors</li> <li>■ Collect all the information necessary for the performance of its supervisory duties</li> </ul>	<ul style="list-style-type: none"> <li>■ Issue warnings and make recommendations to data controllers</li> <li>■ Require a data controller by written notice to give specified information or to produce specified documents which relate to the processing of personal data</li> </ul>	
Board of Directors (ADGM): Its main function is to make rules in respect to personal data processing activities			

### 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?

There are no data protection authorities in the UAE.

In the DIFC, according to Article 26 of the DIFC Law Number 1 of 2007, the commissioner of data protection has the right to prepare draft regulations and standards or codes of practice with respect to data processing activities. This implies that he may have the right to issue a ban on a particular processing activity.

In the ADGM, according to Article 16 of the ADGM 2015 Data Protection Regulations, the Board of Directors may make rules in respect of any matters related to the processing of personal data. This implies that the Board may have the right to issue a ban on a particular processing activity.

### 16.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

The DIFC Law Number 1 of 2007 is largely modelled on the data protection principles emanating from EU Directives, which provide guidance to the DIFC Commissioner of Data Protection in the administration of the DIFC Law Number 1 of 2007. In *Maximilian Schrems v Data Protection Commissioner* [Case no C-362/14] of 6 October 2015, the European Court of Justice invalidated Commission Decision 2000/520/EC which provided protection for personal data transfers from European Union Member States to US Safe Harbor recipients. This has led the DIFC Commissioner of Data Protection to reconsider the adequacy status previously given to transfers of personal data to US Safe Harbor Recipients.

### 16.4 Does the data protection authority ever exercise its powers against companies established in other jurisdictions? If so, how is this enforced?

In the ADGM, according to Article 17 of the ADGM 2015 Data Protection Regulations, if the Registrar is satisfied that a data

controller, data processor or data controller established outside the Abu Dhabi Global Market has contravened or is contravening these regulations or any rules made under these Regulations, the Registrar may issue a direction to the data controller requiring him to do or refrain from doing an act, or to refrain from processing any personal data.

## 17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

### 17.1 How do companies typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

In the mainland of the UAE, in the DIFC and in the ADGM, companies are expected to cooperate with foreign e-discovery requests, although there is no legislation forcing them to do so.

### 17.2 What guidance has/have the data protection authority(ies) issued?

No guidance has been issued on this matter.

## 18 Trends and Developments

### 18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

In January 2018, the Ministry of Finance addressed the importance of protecting sensitive personal data in financial transactions with respect to collecting, processing and retaining personal data.

### 18.2 What “hot topics” are currently a focus for the data protection regulator?

Data available on social media is currently a focus for the data protection regulator, as discussions have emerged on whether such data should be kept private or if it can indeed be used to target advertisements on a particular individual.

## Acknowledgment

The authors would like to thank Jad Doudar, a Paralegal at BSA Ahmad Bin Hezeem & Associates LLP, for his invaluable assistance in the preparation of this chapter.

**Rima Mrad**

BSA Ahmad Bin Hezeem & Associates LLP  
Gate Precinct 3  
DIFC  
P.O. Box 262  
Dubai  
United Arab Emirates

Tel: +971 4 368 5555  
Email: [rima.mrad@bsabh.com](mailto:rima.mrad@bsabh.com)  
URL: [www.bsabh.com](http://www.bsabh.com)

Rima is a Partner with the Corporate and M&A practice, based in our DIFC offices in Dubai. She is an experienced corporate and insurance lawyer who has practised in the UAE for over eight years. Rima specialises in advising insurance companies, corporate organisations, financial institutions, energy companies and private equity funds on a wide range of legal issues including M&A transactions, due diligence, commercial agreements, commercial-related disputes, IT-related transactions and various regulatory matters.

Rima has also advised and assisted international clients in developing their business throughout the GCC, particularly in relation to regulatory and compliance matters and provides employment advice to companies in relation to policies, structuring and breach of contract.

**Nadim Bardawil**

BSA Ahmad Bin Hezeem & Associates LLP  
Gate Precinct 3  
DIFC  
P.O. Box 262  
Dubai  
United Arab Emirates

Tel: +971 4 368 5555  
Email: [nadim.bardawil@bsabh.com](mailto:nadim.bardawil@bsabh.com)  
URL: [www.bsabh.com](http://www.bsabh.com)

Nadim is a Senior Associate in our Corporate and M&A, and Intellectual Property practices based in our DIFC office in Dubai. He specialises in transactional corporate work across various industries including media, technology and healthcare.

Nadim advises on a range of local and international corporate and commercial matters including joint ventures, commercial agency, private equity, employment and regulatory. He has assisted clients with implementing mergers and acquisitions as well as represented clients in the negotiation of IP transfer and licensing provisions.

Nadim is fluent in a number of key languages including English, French and Arabic. Nadim holds a J.D. degree from the Hofstra University School of Law and is admitted to practice in the State of New York. He also holds a business management degree.



BSA Ahmad Bin Hezeem & Associates LLP traces its roots to 2001 when it was first founded in Dubai, with the primary mission of offering legal services that combine comprehensive knowledge of local law with a modernised and progressive approach to legal practice.

Today, following the joining of Senior Partner Dr. Ahmad Bin Hezeem, former Director General of Dubai Courts, and the opening of further offices across the Middle East and now France, we have consolidated our excellence-driven regional reach. Our access to key local authorities and our solid legal expertise across a broad spectrum of industries set us apart as one of the few Dubai-headquartered legal practices that have exceeded their original boundaries.

The growth of BSA is built by teams of innovative legal minds, possessing extensive regional experience and local rights of audience before all courts in the jurisdictions in which we operate, and through the support network of our affiliates in the Middle East and North Africa region (including the GCC), Asia and Europe.



# United Kingdom

Tim Hickman



Matthias Goetz



White & Case LLP

## 1 Relevant Legislation and Competent Authorities

### 1.1 What is the principal data protection legislation?

From 25 May 2018, the principal data protection legislation in the EU will be Regulation (EU) 2016/679 (the “**General Data Protection Regulation**” or “**GDPR**”). The GDPR repeals Directive 95/46/EC (the “**Data Protection Directive**”) and leads 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 introduced in Parliament the UK Data Protection Bill, which covers those areas of the GDPR which EU Member States can add to or vary or that do not fall within EU law. The UK Data Protection Bill is intended to come into force from 25 May 2018.

The GDPR applies in the UK until it leaves the EU, which is expected in March 2019 (“**Brexit**”). The UK Government plans to incorporate the GDPR into the UK’s domestic law as of the leave date under clause 3 of the European Union (Withdrawal) Bill, which incorporates EU law into domestic law and is currently before the UK Parliament. It is expected that after Brexit, data protection law within the UK will be aligned with the GDPR.

### 1.2 Is there any other general legislation that impacts data protection?

The Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended by the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011) (the “**PECR**”) implements the requirements of Directive 2002/58/EC (as amended by Directive 2009/136/EC) (the “**ePrivacy Directive**”). 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 that would harmonise the applicable rules across the EU. The ePrivacy Regulation is still in draft at this stage and is not expected to be passed before 2019.

### 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 GDPR and the PECR. 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 was appointed Information Commissioner.

## 2 Definitions

### 2.1 Please provide the key definitions used in the relevant legislation:

- “**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.
- “**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.
- “**Data Subject**” means an individual who is the subject of the relevant 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**” 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.
- “**Processor**” means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
- “**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.

- *Other key definitions – please specify (e.g., “Pseudonymous Data”, “Direct Personal Data”, “Indirect Personal Data”).*  
There are no other key definitions to specify.

### 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 a 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 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. However, 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)?

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?

This is not applicable in our jurisdiction.

**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; 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 to his or her role as a Data Protection Officer?**

The appointed Data Protection Officer should not be dismissed or penalised for performing its 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 (“DPIAs”) 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”) recommends 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, 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 Data Protection Officer; (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 the 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?)

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. In 2017, the European Commission published a draft of the ePrivacy Regulation which, together with the GDPR, will make it harder to obtain consent.

### 9.2 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 unsolicited marketing calls. However, the UK offers an opt-out register (the Telephone Preference Service (the “TPS”)). It is a legal requirement to not make unsolicited marketing calls to numbers registered in the TPS, unless the business has the consent of the relevant individual to do so.

### 9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

No, they do not.

### 9.4 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. There has been significant focus over the 2016–2018 period on “nuisance calls”. In January 2018, the fines for contacting individuals without their consent ranged from £40,000 to £350,000.

### 9.5 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 of 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.

### 9.6 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.

## 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 Directive 95/46/EC and, from 25 May 2018, the GDPR). For consent to be valid, it must be informed, specific, freely given and must constitute a real 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, which means that it must be essential to fulfil their request.

### 10.2 The EU Commission intends to pass a new ePrivacy Regulation that will replace the respective national legislation in the EU Member States. The regulation is planned to come into force May 25, 2018 and will provide amended requirements for the usage of cookies. Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

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 they have either the consent of the user prior to commencing tracking, or if the information obtained by the tracking is necessary for the delivery of the service. Cookies which do not invade privacy (e.g., those which count the number of visitors to websites) would not require consent. Furthermore, 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?

Between April 2016 and March 2017, the ICO received limited complaints about cookies, and therefore regard cookies as an area of low concern. Between October 2012 and July 2017, the ICO contacted 418 organisations in connection with cookie compliance.

### 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.



## 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) or the business has implemented one of the required safeguards as specified by the GDPR.

### 11.2 Please describe the mechanisms companies 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.

Transfer of personal data to the US is also possible if the data importer has signed up to the EU-US Privacy Shield Framework, which was designed by the US Department of Commerce and the EU Commission to provide businesses in the EU and the US with a mechanism to comply with data protection requirements when transferring personal data from the EU to the US.

### 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.

## 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. The WP29 recommends 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.

### 12.2 Is anonymous reporting prohibited, or 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, the WP29 considers 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 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 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.

**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, e.g., if a CCTV camera is used for the purpose of monitoring criminal activity in an office, it cannot also be used for monitoring the work attendance of employees.

**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. Generally, any adverse impact on the employees must be justified by the benefits of the employer. Employers must consider whether the monitoring methods are too intrusive, such that its 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 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 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 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 Power	Civil/Administrative Sanction	Criminal Sanction
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 of 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.	N/A
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).	N/A
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.	N/A

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
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.	N/A
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.	N/A

#### 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 ICO tends to co-operate with businesses before it takes enforcement action. Although unlikely, the ICO may take a different approach to the enforcement of 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 GDPR can also apply to non-EU businesses even if they have no physical presence in the EU (see the answer to question 3.1 above). Such businesses must appoint a representative in the EU against which the ICO or the relevant data protection authority can take relevant enforcement action under the GDPR.

### 17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

#### 17.1 How do companies typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

There is no EU standard response.

#### 17.2 What guidance has/have the data protection authority(ies) issued?

There is no standalone guidance on this point.

## 18 Trends and Developments

### 18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

In 2016, the ICO issued its largest ever fine of £400,000 under the UK Data Protection Act 1998 against the telecoms company TalkTalk for security failings that allowed a cyber attacker to access customer data. The GDPR allows for much higher fines, and it is expected that the ICO will issue these in the future.



**Tim Hickman**

White & Case LLP  
5 Old Broad Street  
London EC2N 1DW  
United Kingdom

Tel: +44 7532 2517  
Email: [tim.hickman@whitecase.com](mailto:tim.hickman@whitecase.com)  
URL: [www.whitecase.com](http://www.whitecase.com)

Tim advises on all aspects of UK and EU privacy and data protection law, from general compliance issues (such as implementing privacy policies and consent forms) to more specialised issues (such as managing data breaches, structuring cross-border data transfers and complying with the “right to be forgotten”). Tim has a detailed knowledge of the EU’s General Data Protection Regulation, and co-authored White & Case’s Handbook on that legislation ([www.whitecase.com/eu-gdpr-handbook](http://www.whitecase.com/eu-gdpr-handbook)).

Clients appreciate Tim’s ability to find pragmatic and commercial solutions to complex (and frequently multi-jurisdictional) data protection compliance questions.

Tim has significant experience of working with a wide range of clients in the EU, the US and Asia. He has also spent time on secondment at Google, advising on cutting-edge privacy and data protection issues.

### 18.2 What “hot topics” are currently a focus for the data protection regulator?

In January 2018, a number of fines were issued by the ICO for contravention of electronic direct marketing regulations. The largest was to Miss-sold Products UK Ltd, which was fined £350,000 for failing to ensure marketing calls were made only to individuals who had consented. These incidents attracted a large amount of media attention, and it would appear that breaches are set to remain an important area of interest for the ICO.



**Matthias Goetz**

White & Case LLP  
5 Old Broad Street  
London EC2N 1DW  
United Kingdom

Tel: +44 7532 2574  
Email: [matthias.goetz@whitecase.com](mailto:matthias.goetz@whitecase.com)  
URL: [www.whitecase.com](http://www.whitecase.com)

Matthias is an associate in the Global Intellectual Property Practice of the law firm White & Case LLP in London. He advises national and international companies in the areas of data protection and privacy, information technology (IT) and intellectual property (IP), including IP and data protection aspects of corporate transactions.

In the area of data protection and privacy, he advises on matters such as cross-border data transfers, data breach responses, implementing privacy policies, and general data protection compliance issues. Matthias advises numerous clients on the likely impact of the EU’s General Data Protection Regulation. He also advises a major global bank on various commercial contracts, including services agreements, software licence and support agreements, and outsourcing agreements.

## WHITE & CASE

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, manufacturing and electronics, publishing and media.

# USA

Pillsbury Winthrop Shaw Pittman LLP

Deborah Thoren-Peden



Catherine D. Meyer



### 1 Relevant Legislation and Competent Authorities

#### 1.1 What is the principal data protection legislation?

The protection of data of US residents is regulated by laws enacted on both the national and the state level. There is no single principal data protection legislation. Federal statutes are primarily aimed at specific sectors, as described more fully below, while state statutes are more focused on protecting the privacy rights of individual consumers. The right to privacy is a common law right that has been incorporated into the state constitutions of many states and into the laws at both the state and federal level. Laws protecting data and consumer privacy are based on the principle that an individual has an expectation of privacy unless that expectation has been diminished or eliminated by agreement, statute or disclosure. Data protection and privacy statutes in the US are enacted to protect the individuals residing in the US or one of its states. Federal laws apply to protect residents of all states. State laws are designed to protect their residents.

#### 1.2 Is there any other general legislation that impacts data protection?

Most states have adopted laws protecting the personally identifiable information of their residents. These laws apply to the information about a resident of the particular state and require businesses to comply with the state's laws if the business collects, holds, transfers or processes information about a state resident, even if the business does not have a physical presence or business operation in the state.

The type of information protected varies depending on the statute. Some statutes apply to any information that relates to an identifiable individual while some apply to a more limited set of personally identifiable information – an individual's name together with a data element such as a Social Security Number, driver's licence number, financial account number, and medical or health information. A growing number of states include protection of biometric data under these laws.

These state laws may include an obligation:

- to protect personal information from unauthorised access, misuse or destruction;
- to take reasonable steps to securely destroy records containing personal information when it is to be discarded so that the information is rendered undecipherable;
- to protect Social Security Numbers against public disclosure;

- to restrict the collection and use of driver's licence information for any purpose other than age verification or identification;
- to provide written notification to any data subject whose sensitive personal information is accessed or acquired by an unauthorised person;
- to require vendors or service providers to protect data shared with them;
- to restrict the sale of email addresses;
- to restrict the collection of personal information in certain types of transactions;
- to adopt comprehensive written data security plans; and
- to encrypt personal information in transmission over the internet or in storage on portable devices.

Not all states have enacted all such laws and where multiple states address a specific topic, the laws in those states are not necessarily consistent with each other, but vary from state to state. Some states, like California, are more active in protecting its consumers, restricting disclosure of personal information for marketing purposes, requiring online privacy disclosures and granting minor children the right to be forgotten in their online postings. Massachusetts, for example, has strong data protection regulations (201 CMR 1700), requiring any entity that holds, transmits or collects "personal information" of a Massachusetts resident to implement and maintain a comprehensive written data security plan addressing 12 designated activities. New York has adopted Cyber Security Regulations applicable to financial institutions doing business in the state which require comprehensive plans to address cyber security risks.

A number of states restrict the collection of data from consumers, generally in the context of retail transactions with customers. These include limiting information that can be collected in a credit card or cheque transaction.

Most states have enacted legislation that restricts recording communications involving telephones (wiretap laws) or offline (eavesdropping laws) without obtaining consent from one or all parties. These laws apply to any call initiated in or connecting to a phone in the state, and some carry criminal penalties.

Finally, some states have enacted laws specifically protecting children residing in the state. These include Child Protection Registry laws which prohibit sending any child under the age of 18 to contact points listed with the registry communications promoting any product which the child is legally not permitted to own, purchase, view, possess or use; and requiring operators of online sites that allow children under the age of 18 to post information about themselves to provide the minors a means of deleting all such information upon request.



### 1.3 Is there any sector-specific legislation that impacts data protection?

Historically, US federal law has regulated data protection and consumer privacy on a sectoral basis, focusing specific regulations on financial services and health care providers. In addition, federal law imposes obligations on businesses generally to prohibit unfair or deceptive practices, to protect the intrusive use of consumer information when considering eligibility for insurance, employment or credit, and to regulate telephone, text, fax and email marketing.

The Gramm Leach Bliley Act (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 on financial service industry companies requirements for securing NPI, restricting disclosure and use of NPI and notifying customers when NPI is improperly exposed to unauthorised persons.

The Health Information Portability and Accountability Act (29 U.S. Code 1181 *et seq.*) protects information held by a covered entity that concerns health status, provision of health care or payment for health care 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.

Under the Federal Trade Commission Act (15 U.S. Code 41 *et seq.*), the US Federal Trade Commission (FTC) is broadly empowered 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.

The Driver’s Privacy Protection Act of 1994 (18 U.S. Code 2721 *et seq.*) governs the privacy and disclosure of personal information gathered by state Departments of Motor Vehicles. The DPPA restricts how personal information is released. The DPPA defines personal information as information that identifies a person including photographs, Social Security Number (SSN), Client Identification Number (CID), name, address (but not the five-digit ZIP code), telephone number, medical information and disability information.

The Fair Credit Reporting Act, as amended by Fair and Accurate Credit Transactions Act (FACTA) (15 U.S. Code 1681), restricts use of information bearing on an individual’s credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living to determine eligibility for credit, employment or insurance. It also requires truncating credit card numbers on printed credit card receipts, requires securely destroying certain types of personal information and regulates the use of

certain types of information received from affiliated companies for marketing purposes. Finally, it imposes obligations on financial institutions and creditors to institute programmes that detect and respond to instances of identity theft under its Identity Theft Red Flag Rule.

Unsolicited commercial emails are regulated under the CAN-SPAM Act (15 U.S. Code 7704), which requires certain technical information to be included in unsolicited emails and permits consumers to opt-out of the receipt of such emails.

The Telephone Consumer Protection Act (TCPA) and associated regulations regulate all calls and text messages to mobile phones and regulate calls to residential phones that are made for marketing purposes or using automated dialing systems or prerecorded messages under its Telemarketing Sales Rule.

Children’s information is protected at the federal level under the Children’s Online Privacy Protection Act (COPPA) (15 U.S. Code 6501), which prohibits the online collection of any information from a child under the age of 13, 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.*) was enacted to protect wrongful disclosure of video-tape rental or sale records or similar audio-visual materials, including online streaming.

Generally, where a federal statute covers a specific topic, the federal law pre-empts any similar state law on that topic. However, certain federal laws, like the Gramm Leach Bliley Act, for instance, specifies that it is not pre-emptive of state laws on the subject. As a result, some states have enacted sectoral laws similar to those federal statutes listed above, with some of those state laws being more restrictive than the federal laws.

### 1.4 What authority(ies) are responsible for data protection?

At the federal level, the FTC, the Office of the Comptroller of the Currency, and the Department of Health and Human Services.

## 2 Definitions

### 2.1 Please provide the key definitions used in the relevant legislation:

#### ■ “Personal Data”

The definition of personal information in the US is not uniform across all states or all regulations. In addition, certain data may be considered to be personal information for one purpose but not for another. The breadth of the definition varies by statute as illustrated by the following chart referencing California statutes as examples.

	First and last name	Home or physical address (street and city)	Email address	Telephone number	Social security number	Identifier allowing for physical or online contact	Signature	Passport number	Driver's license number/ State issued ID	Physical characteristics or description	Insurance policy number	Education	Employment	Financial Account number	Medical information	Health insurance information	Information capable of being associated with a particular individual	User name email plus password for online account	Height, weight, gender, religion, political party affiliation, age, date of birth	Children's names, age, gender, number, email addresses
California Online Privacy Protection Act	X	X	X	X	X	X														
California Data Destruction Statute	X	X		X	X		X	X	X	X	X	X	X	X	X	X	X			
California Data Protection Statute	X with data point				X				X					X	X	X		X		
California Data Breach Notification Statute	X with data point				X				X					X	X	X		X		
California Disclosure of personal information for marketing purposes statute	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

- **“Processing”**  
This is not applicable.
- **“Controller”**  
This is not applicable.
- **“Processor”**  
This is not applicable.
- **“Data Subject”**  
The state data protection statutes reference either individuals residing within the state or a “consumer” residing within the state. A “consumer” is an individual who engages with a business for personal, family or household purposes.
- **“Sensitive Personal Data”**  
This is not applicable.
- **“Data Breach”**  
The definition of Data Breach depends on the individual statute.
- *Other key definitions – please specify (e.g., “Pseudonymous Data”, “Direct Personal Data”, “Indirect Personal Data”)*  
This is not applicable.

### 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 are subject to federal data protection laws for all US residents and also to state data protection laws, based on the state of residence of any individual whose information the business collects, holds, transmits, processes or shares. This is based on a long-established principle articulated by the US Supreme Court in 1954 that a state “may regulate to protect interests of its own people, even though other phases of the same transactions might justify regulator legislation in other states” (*Watson v. Employer Liability Corp.* (1954) 348 U.S. 66 at 72). While each state may not regulate businesses that are entirely outside of it and have no contact with residents of the state, when a business interacts with the residents of a state, each state has a legitimate interest in protecting the health, life and safety of its citizens. Data protection falls under this principle.

## 4 Key Principles

### 4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**  
US data protection statutes are focused generally on security of the data. As such, the European principles of transparency, lawful basis for processing, purpose limitation, data minimisation, proportionality and data retention are not addressed in the statutes. We note that there is guidance regarding a minimum period of time in which certain documents, like employee records, must be retained, but there is not necessarily a requirement for the destruction of those records after that time has expired. This is left to a company’s decision.
- **Lawful basis for processing**  
This is not applicable.
- **Purpose limitation**  
This is not applicable.
- **Data minimisation**  
This is not applicable.
- **Proportionality**  
This is not applicable.
- **Retention**  
This is not applicable.
- *Other key principles – please specify*  
This is not applicable.

## 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 certain circumstances, employees are entitled to receive copies of data held by employers. Parents are entitled to receive copies of information collected online from children under the age of 13. Under the Health Insurance Portability and Accountability Act (HIPAA), individuals are entitled to request copies of medical information held by a health services provider. Under the Fair Credit Reporting

Act, individuals are permitted to receive a copy of consumer report information that is maintained by a consumer reporting agency.

■ **Right to rectification of errors**

This is not applicable.

■ **Right to deletion/right to be forgotten**

One state (California) permits individuals to request deletion of information posted online while under the age of 18.

■ **Right to object to processing**

At the federal level, 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 Telephone Consumer Protection Act. At the state level, individuals have 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**

This is not applicable.

■ **Right to data portability**

Under the Health Insurance Portability and Accountability Act (HIPAA), individuals are entitled to request that medical information held by a health services provider be transferred to another health services provider.

■ **Right to withdraw consent**

Under the Telephone Consumer Protection Act, individuals are permitted to withdraw consent given to receive certain types of calls to residential or mobile telephone lines.

■ **Right to object to marketing**

Under CAN-SPAM, individuals are permitted to opt-out of receiving commercial (advertising) emails. Under the Telephone Consumer Protection Act, 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 of what information is shared and with whom.

■ **Right to complain to the relevant data protection authority(ies)**

This is not applicable.

■ *Other key rights – please specify*

This is not applicable.

## 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.**

Certain statutes require the appointment or designation of an individual or individuals who are charged with compliance with the statute. These include the Gramm Leach Bliley Act, 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 enforcement action by the relevant regulator.

- 7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect to 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?**

The designated individual must be an employee of the entity for which it acts.

- 7.5 Please describe any specific qualifications for the Data Protection Officer required by law.**

This is not specified.

- 7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?**

General oversight of compliance with the regulation.

- 7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?**

No, this is not a requirement.

- 7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?**

No, this is not a 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?**

Under the laws of certain states, 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. The form of the contract is not specified.

- 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.)?**

See above.

## 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 Telephone Consumer Protection Act before marketing calls or texts may be sent to a mobile telephone line. Certain disclosures are required to be given regarding whether the calls will be made using an automatic dialing machine or a pre-recorded voice message, whether a purchase is required, and whether there is a charge for the text. The same statute authorised the establishment of the national Do-Not-Call list which allows individuals to submit their telephone numbers to a national registry inclusion which prohibits marketing calls to such number.

Other federal statutes do not require opt-in consent, just the provision of an opt-out. For instance, under CAN-SPAM, marketing emails 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 that remains operational for 60 days, and the sender honours opt-outs within 10 days of receipt.

- 9.2 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 Telephone Consumer Protection Act. This regulation established the national Do-Not-Call list of telephone numbers that cannot be used for marketing calls and disclosure requirements for companies engaging in telephone marketing. It also proscribes limitations on the use of telephone marketing, including, for instance, limiting times when marketing calls may be placed, 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 the mail.

It should be noted that the Federal Trade Commission Act, which regulates deceptive practices, has been used to enforce, as a deceptive practice, 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 have deceptive practices statutes that are used to impose penalties or injunctive relief in similar circumstances, or where violation of a federal statute is deemed to be a deceptive practice under state law.

**9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?**

Yes, if the recipient is within the United States.

**9.4 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?**

The FTC and the Attorneys General of the states are active in enforcement in this area.

**9.5 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 must 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.

**9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?**

The penalties under CAN-SPAM are \$16,000 per email for an isolated or unintentional violation; penalties can increase to the current maximum of \$41,484 (as of 2018) for flagrant or repeated violations. The penalties under the Telephone Consumer Protection Act are \$500 for each text message or call sent in violation of the Act, the amount of which may be trebled in the case of intentional or flagrant violations. By way of example, the FTC and the attorneys general of several states obtained a judgment of \$260 million in 2017 for violation of the Telephone Consumer Protection Act.

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 Consumer Fraud and Abuse Act has been used as the basis for enforcement actions against companies that use cookies for behavioural advertising, where the cookie enables deep packet inspection of the computer on which it is placed. At least one state (California) requires disclosures to be made where cookies are used to collect information about a consumer's online activities across different websites or over time.

In addition, the Federal Trade Commission Act and state deceptive practices acts have been used as the basis for regulatory enforcement and private class action lawsuits against companies that failed to disclose or misrepresented their use of tracking cookies. One such action was settled in 2012 with a payment of \$22.5 million to the FTC; the same company agreed in 2016 to pay \$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 comes into play where cookies collect information from the computer on which they are placed and report that information to the entity placing the cookies.

**10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?**

Yes, on both the regulatory side through the FTC and on the privacy side through class action lawsuits.

**10.4 What are the maximum penalties for breaches of applicable cookie restrictions?**

Maximum penalties 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 US does not place restrictions on the transfer of personal data to other jurisdictions.

**11.2 Please describe the mechanisms companies 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.

**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, they do not.

**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 a Federal Whistle-blower Protection Act protecting federal employees, and some states have similar statutes protecting state



employees. Public companies subject to the Sarbanes-Oxley Act are required to have a Whistle-blower Policy which must be approved by the board of directors and include a definition of whistle-blowing, the individuals covered, non-retaliation provisions, confidentiality, processes and enforcement measures.

**12.2 Is anonymous reporting prohibited, or strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do companies typically address this issue?**

This is not specified.

## 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 state criminal eavesdropping statutes which require posting signs where video monitoring is taking place.

**13.2 Are there limits on the purposes for which CCTV data may be used?**

The limitations would be based on the expectation of privacy that remains following disclosure of the CCTV recording by the company employing it, and any other policies issued by the company relating to data collected by this process.

## 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 agreement, statute or disclosure. Monitoring of employees is permitted where the employer makes clear disclosure regarding the type and scope of monitoring in which it engages.

**14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.**

Notice to employees is required in order to diminish their expectation of privacy.

**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.)?**

Certain federal statutes and certain individual state statutes impose an obligation to ensure security of personal information. The Federal Gramm Leach Bliley Act and HIPAA impose such requirements on financial services and covered health care entities. Some states impose data security obligations on any entities that collect, hold or transmit limited types of personal information.

**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) expects voluntary breach reporting.**

At the federal level, data breach notification requirements are imposed under the Privacy Act (applicable to federal government agencies), the Federal Information Security Management Act (applicable to federal government agencies), the Office of Management and Budget Guidance (applicable to federal government agencies), the Veterans Affairs Information Security Act (applicable to the Department of Veterans Affairs), the Health Insurance Portability and Accountability Act (applicable to health plans, health care clearing houses, and health care providers who transmit financial and administrative transactions electronically and their business associates), the Health Information Technology for Economic and Clinical Health Act (applicable to health plans, health care clearing houses, and health care providers who transmit financial and administrative transactions electronically and their business associates), and the Gramm-Leach-Bliley Act (applicable to financial institutions and financial services entities).

HIPAA requires reporting an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information to the Department of Health and Human Services. 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, requires public companies to provide notification through filings with the Securities and Exchange Commission when material events, including cyber incidents, occur. Registrants are required to disclose conclusions on the effectiveness of disclosure controls and procedures. 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 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 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. Some states require agency notification within a very short period of time (for example, New Jersey: 48 hours).

**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) expects voluntary breach reporting.**

The Gramm Leach Bliley Act requires financial institutions and financial services entities to promptly report data breaches as defined in that Act to impacted individuals where a risk of harm is presented. HIPAA requires covered entities to report to impacted individuals, within 60 days, data breaches as defined in that statute.

As of May 2018, all 50 states, the District of Columbia, Guam, Puerto Rico and the US Virgin Islands have statutes that require reporting data breaches 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 data, but some states include personal data in any format. Triggering personal data 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 or financial account number. Some states include data of birth, mother’s maiden name, passport number, biometric data, employee identification number or user name and password as additional triggering data points. Standards for when disclosure is required vary from unauthorised access to personal information, to unauthorised acquisition of personal data, to misuse of or risk of harm to personal information. Most states require notification to be given as soon as practical, but at least one state (Florida) requires disclosure within 30 days of discovery of the incident and others within 45 days of discovery. 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 the 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?**

Not all states impose financial penalties for failure to report data security breaches, but Florida, for instance, can impose penalties of up to \$500,000 for such a failure to timely report.

## 16 Enforcement and Sanctions

**16.1 Describe the enforcement powers of the data protection authority(ies).**

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
See below.		

**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 US does not have a central data protection authority. Authority to enforce is specified in the relevant statutes. Some include only 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.

**16.3 Describe the data protection authority’s approach to exercising those powers, with examples of recent cases.**

This depends on the relevant statutory enforcement mechanism and the agency conducting the enforcement measures.

**16.4 Does the data protection authority ever exercise its powers against companies established in other jurisdictions? If so, how is this enforced?**

Extraterritorial enforcement of a US law would depend on a number of factors including whether the entity is subject to the jurisdiction of the US courts, the impact on US commerce and the impact on US residents, among other factors.

## 17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

**17.1 How do companies typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?**

Typically, such requests must be processed through the local courts or law enforcement.

**17.2 What guidance has/have the data protection authority(ies) issued?**

Since there is no central data protection authority, and since the agencies tasked with enforcement of certain statutes also enforce non-data protection issues there is no central repository of guidance. By way of example, the FTC has issued guidance on a variety of issues including children’s privacy, identity theft and telemarketing. State Attorneys General have, in some cases, offered resources on their websites for victims of identity theft and for companies suffering data security breaches. The Department of Health and Human Services has issued information on compliance with HIPAA.

## 18 Trends and Developments

### 18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

The FTC remains active in enforcing deceptive practices including those involving marketing and security, though not specifically in the area of data protection. The DHHS remains active in enforcing

HIPAA violations. Class action lawsuits alleging improper telephone recording and text messaging remain active, particularly where the statute includes a minimum financial penalty.

### 18.2 What “hot topics” are currently a focus for the data protection regulator?

See above.



#### Deborah Thoren-Peden

Pillsbury Winthrop Shaw Pittman LLP  
725 South Figueroa Street  
Los Angeles  
CA 90017  
USA

Tel: +1 213 488 7320  
Email: [deborah.thoren-peden@pillsburylaw.com](mailto:deborah.thoren-peden@pillsburylaw.com)  
URL: [www.pillsburylaw.com](http://www.pillsburylaw.com)

**Deborah Thoren-Peden** focuses her practice on privacy, banking, e-commerce, anti-money laundering and Office of Foreign Assets Control regulations. She co-leads the firm's Cybersecurity, Data Protection & Privacy team. Ms. Thoren-Peden advises a spectrum of industries on the laws and regulations related to privacy, data mining, and the ability to use such information for marketing purposes and share it with others. She has prepared numerous privacy policies and procedures for a wide variety of companies, both domestic and international. She was the Chief Privacy Officer of PayMyBills.com and served on the Privacy Task force of the American Bankers Association.



#### Catherine D. Meyer

Pillsbury Winthrop Shaw Pittman LLP  
725 South Figueroa Street  
Los Angeles  
CA 90017  
USA

Tel: +1 213 488 7362  
Email: [catherine.meyer@pillsburylaw.com](mailto:catherine.meyer@pillsburylaw.com)  
URL: [www.pillsburylaw.com](http://www.pillsburylaw.com)

**Catherine D. Meyer** is recognised by *The Legal 500 U.S.* as an authority on data protection, privacy and cyber law. Her practice includes: advising individuals and businesses on financial privacy rights and compliance; protecting customers' privacy under state, federal and international statutes and regulations; assisting clients when personal information is compromised or threatened; and responding to data breaches. Well versed in regulations regarding the collection, use, sale, transfer and sharing of customer information for commercial purposes, Ms. Meyer regularly counsels on marketing issues applicable to various communications channels and compliance with international privacy directives.

pillsbury

**Pillsbury** is a leading international law firm with 700+ lawyers located around the world. The firm has been recognised as one of the Most Innovative Law Firms by *Financial Times* three years running, and is one of the 25 law firms most frequently recommended by general counsel according to a 2016 BTI Consulting Group survey. Recognised by *The Legal 500* as one of the world's foremost practices, Pillsbury offers unparalleled experience and knowledge in connection with critical cyber security, data protection and privacy law issues. Pillsbury has advised businesses on all manner of data privacy issues. Our uncommon insight, combined with an expansive network of government and regulatory connections at the highest levels, affords clients unparalleled resources for navigating and tackling their data-related challenges.

## NOTES

---





### Other titles in the ICLG series include:

- Alternative Investment Funds
- Anti-Money Laundering
- Aviation Law
- Business Crime
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Copyright
- Corporate Governance
- Corporate Immigration
- Corporate Investigations
- Corporate Recovery & Insolvency
- Corporate Tax
- Cybersecurity
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Fintech
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Investor-State Arbitration
- Lending & Secured Finance
- Litigation & Dispute Resolution
- Merger Control
- Mergers & Acquisitions
- Mining Law
- Oil & Gas Regulation
- Outsourcing
- Patents
- Pharmaceutical Advertising
- Private Client
- Private Equity
- Product Liability
- Project Finance
- Public Investment Funds
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks
- Vertical Agreements and Dominant Firms



59 Tanner Street, London SE1 3PL, United Kingdom  
Tel: +44 20 7367 0720 / Fax: +44 20 7407 5255  
Email: [info@glgroup.co.uk](mailto:info@glgroup.co.uk)

[www.iclg.com](http://www.iclg.com)