The information provided in this publication is general and may not apply in a specific situation, nor does it necessarily represent the views of authors' firms or their clients. Legal advice should always be sought before taking any legal action based on the information provided. The publishers accept no responsibility for any acts or omissions contained herein. Although the information provided is accurate as of September 2018, be advised that this is a developing area.

Enquiries concerning reproduction should be sent to Law Business Research, at the address above.

Enquiries concerning editorial content should be directed to the Publisher – tom.barnes@lbresearch.com


Printed in Great Britain by Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

© 2018 Law Business Research Ltd
ACKNOWLEDGEMENTS

The publisher acknowledges and thanks the following for their learned assistance throughout the preparation of this book:

ALLENS
ASTREA
BOGSCH & PARTNERS LAW FIRM
BTS&PARTNERS
JUN HE LLP
KOBYLAŃSKA & LEWOSZEWSKI KANCELARIA PRAWNA SP J
M&MBOMCHIL
MÁRQUEZ, BARRERA, CASTAÑEDA & RAMÍREZ
MATHESON
MATTOS FILHO, VEIGA FILHO, MARREY JR E QUIROGA ADVOCADOS
NOVATION LLP
NOERR
SANTAMARINA Y STETA, SC
SIDLEY AUSTIN LLP
SK CHAMBERS
SUBRAMANIAM & ASSOCIATES
URÍA MENÉNDEZ ABOGADOS, SLP
WALDER WYSS LTD
WINHELLER RECHTSANWALTSGESELLSCHAFT MBH
# CONTENTS

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>GLOBAL OVERVIEW</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Alan Charles Raul</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>EUROPEAN UNION OVERVIEW</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>William RM Long, Géraldine Scali, Francesca Blythe and Alan Charles Raul</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>APEC OVERVIEW</td>
<td>40</td>
</tr>
<tr>
<td></td>
<td>Ellyce R Cooper and Alan Charles Raul</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>ARGENTINA</td>
<td>53</td>
</tr>
<tr>
<td></td>
<td>Adrián Lucio Furman, Mercedes de Artaza and Francisco Zappa</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>AUSTRALIA</td>
<td>64</td>
</tr>
<tr>
<td></td>
<td>Michael Morris</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>BELGIUM</td>
<td>77</td>
</tr>
<tr>
<td></td>
<td>Steven De Schrijver</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>BRAZIL</td>
<td>98</td>
</tr>
<tr>
<td></td>
<td>Fabio Ferreira Kajawski and Alan Campos Elias Thomaz</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>CANADA</td>
<td>109</td>
</tr>
<tr>
<td></td>
<td>Shaun Brown</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>CHINA</td>
<td>125</td>
</tr>
<tr>
<td></td>
<td>Mariissa (Xiao) Dong</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>COLOMBIA</td>
<td>136</td>
</tr>
<tr>
<td></td>
<td>Natalia Barrera Silva</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>GERMANY</td>
<td>146</td>
</tr>
<tr>
<td></td>
<td>Olga Stepanova</td>
<td></td>
</tr>
<tr>
<td>Chapter</td>
<td>Country</td>
<td>Authors</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>12</td>
<td>HONG KONG</td>
<td>Yuet Ming Tham</td>
</tr>
<tr>
<td>13</td>
<td>HUNGARY</td>
<td>Tamás Gödölle</td>
</tr>
<tr>
<td>14</td>
<td>INDIA</td>
<td>Aditi Subramaniam and Sanuj Das</td>
</tr>
<tr>
<td>15</td>
<td>IRELAND</td>
<td>Anne-Marie Bohan</td>
</tr>
<tr>
<td>16</td>
<td>JAPAN</td>
<td>Tomoki Ishiara</td>
</tr>
<tr>
<td>17</td>
<td>MALAYSIA</td>
<td>Shanthi Kandiah</td>
</tr>
<tr>
<td>18</td>
<td>MEXICO</td>
<td>César G Cruz-Ayala and Diego Acosta-Chin</td>
</tr>
<tr>
<td>19</td>
<td>POLAND</td>
<td>Anna Kobylańska, Marcin Lewiszewski, Maja Karczewska and Aneta Miskowiec</td>
</tr>
<tr>
<td>20</td>
<td>RUSSIA</td>
<td>Vyacheslav Khayryuzov</td>
</tr>
<tr>
<td>21</td>
<td>SINGAPORE</td>
<td>Yuet Ming Tham</td>
</tr>
<tr>
<td>22</td>
<td>SPAIN</td>
<td>Leticia López-Lapuente and Reyes Bermejo Bosch</td>
</tr>
<tr>
<td>23</td>
<td>SWITZERLAND</td>
<td>Jürg Schneider, Monique Sturny and Hugh Reeves</td>
</tr>
<tr>
<td>24</td>
<td>TURKEY</td>
<td>Batu Kınıkoğlu, Selen Zengin and Kaan Can Akdere</td>
</tr>
</tbody>
</table>
## Contents

<table>
<thead>
<tr>
<th>Chapter</th>
<th>UNITED KINGDOM</th>
<th>William RM Long, Géraldine Scali and Francesca Blythe</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Chapter 25</td>
<td>350</td>
</tr>
<tr>
<td>Appendix 1</td>
<td>ABOUT THE AUTHORS</td>
<td>405</td>
</tr>
<tr>
<td>Appendix 2</td>
<td>CONTRIBUTING LAW FIRMS’ CONTACT DETAILS</td>
<td>419</td>
</tr>
<tr>
<td>Chapter</td>
<td>UNITED STATES</td>
<td>Alan Charles Raul and Vivek K Mohan</td>
</tr>
<tr>
<td>---------</td>
<td>----------------</td>
<td>------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Chapter 26</td>
<td>376</td>
</tr>
<tr>
<td></td>
<td>Appendix 2</td>
<td>419</td>
</tr>
</tbody>
</table>
2018 has been a watershed year for the privacy field. This overview highlights some of the year’s key developments that are discussed in detail in the succeeding chapters.

Obviously, the European Union’s General Data Protection Regulation (GDPR) has been the main attraction. Companies subject to the GDPR have expended and will continue to expend enormous efforts and funds to understand and diagram their data-processing operations. They have also needed to design rigorous new compliance mechanisms, and to implement elaborate systems for providing data subject rights such as access, deletion, rectification and portability.

Now that the GDPR has gone live, as of 25 May 2018, it remains to be seen how the Member State data protection authorities will deploy their significant new penalty authority to enforce substantially more stringent standards. Will US tech companies continue to bear the brunt of EU enforcement wrath, or will the DPAs scrutinise inwards as well?

The world will also be watching to see whether enforcement by the various EU DPAs conforms to acceptable standards of transparency, fairness, due process and consistency. With potential penalties of up to 4 per cent of a company’s global turnover at stake, it is likely that the new European Data Protection Board (EDPB) will have its work cut out to harmonise the data protection policies of increasingly fractious national governments. Will the full range of EU DPAs have the resources, legal authority and administrative experience to enforce the GDPR both fully and fairly?

Perhaps most importantly, will it turn out that the GDPR was worth it?

Given the burdens of complying with the GDPR and the potential for inhibiting technological and commercial innovation, will Europe’s citizens be better or worse off under the GDPR? The correct judgement on this crucial point will depend on whether the privacy benefits of GDPR will outweigh its costs.

One hopes that someone is really paying attention to this question. It will require the acquisition of significant amounts of relevant empirical data to answer it. While privacy and data protection are fundamental rights in the European Union – as they are in most of the world – no society has concluded that privacy rights are absolute. Accordingly, the European Union’s citizens will be well served if EU officials make the effort to monitor the full spectrum of GDPR costs and benefits, and then assess those impacts against the actual privacy risks the GDPR prevents or penalises.

---

1 Alan Charles Raul is a partner at Sidley Austin LLP.
In the United States, privacy regulation has also taken flight – in California. The ‘Golden State’ has adopted the California Consumer Privacy Act (CCPA). That statute will, in January 2020, become by far the most prescriptive privacy law in the United States (not counting federal financial, health, telecom and children’s privacy laws).

The CCPA focuses on requiring explanation and transparency of data collection practices and data uses by companies operating in California (or processing the data of California residents). However, the CCPA is arguably somewhat more reasonable and less restrictive than the GDPR. The CCPA turns primarily on ‘opt-out’ rather than the GDPR’s abiding preference for ‘opt-in’. Moreover, the CCPA does not require burdensome logging of data-processing practices, and does not authorise enormous potential penalties or private litigation (except with regard to data breaches involving exfiltration of personal data). To be sure, however, the CCPA does authorise data subject rights similar to those of the GDPR, namely access, deletion and portability. Time will tell whether the CCPA constrains technological innovation as much as the GDPR certainly will. A final point to consider is that the CCPA may yet be subject to further legislative amendment prior to its 1 January 2020 date, and will in addition be subject to interpretative regulations by the state’s Attorney General.

California is not the only US jurisdiction moving on privacy. Besides new legislation in other states, the cities of San Francisco and Chicago have also taken steps in the direction of regulating privacy and data protection at the municipal level. While little may come of the local policy idiosyncrasies, (and the CCPA would largely pre-empt the San Francisco ordinance), all this policymaking activity has inspired the federal government to consider proposing its own privacy legislation. Federal standards could pre-empt or obviate states from going in 50 different directions (as they have done on data breach notification laws).

At the time of writing, the White House had not yet released its privacy proposals, but they are expected to be published before 2019. In the meantime, the Federal Trade Commission (FTC) has embarked on a substantial series of hearings to examine privacy, big data, artificial intelligence and numerous other consumer protection and competition issues. The FTC is likely to consider very closely what ‘information injuries’ are sufficiently concrete to justify regulatory restriction or enforcement penalties in the realm of alleged privacy or data protection violations. Unlike the European Union, in the United States sanctions are typically only imposed or authorised where the injury at issue is (1) concrete and particularised (i.e., experienced by specific individuals) and (2) de facto and real, rather than wholly abstract. While the United States recognises that intangible injuries may be real and not merely abstract, it will not necessarily be possible to predicate enforcement or private litigation on pure dignitary harm or mild emotional distress. Illusory, trivial or technical privacy harms would not generally support regulation or penalties.

India’s Supreme Court recently held that privacy is a fundamental human right, and the national government is actively considering a comprehensive privacy and data protection regime. India’s proposed new privacy framework is now embodied in draft legislation, which is open for public comment until 30 September 2018. The proposed law appears to follow the EU regime closely. If it is ultimately enacted in this form, we will see whether the new India law enhances or impedes India’s rise as a major hub of technological innovation and digital commerce. India is also considering possible data localisation requirements for storage of personal data in-country and use of local service providers. This could obviously have international trade repercussions.

For the United Kingdom, the key data protection will be – as it will be for many regulatory policy issues – Brexit. In April 2018, the Information Commissioner, Elizabeth
Denham, stated that the Information Commissioner’s Office (ICO) is preparing for the post-Brexit environment, ‘in order to ensure that the information rights of UK citizens are not adversely affected’ by Brexit.

In the meantime, the UK Data Protection Act 2018 came into force on 23 May 2018. It repealed the 1998 UK Data Protection Act, and introduced certain specific derogations that specify how the GDPR applies in UK law. The Act also addressed certain national security privacy provisions, as well as the powers and obligations of the ICO. The ICO has published extensive guidance on the GDPR.

China continues to release numerous national standards regarding cybersecurity for public comment. These regulatory provisions include ‘Measures on Security Assessment of the Cross-Border Transfer of Personal Information and Important Data’ (which incorporate requirements regarding data localisation and security) as well as the ‘Regulations on Security Protection of Critical Information Infrastructures’. Certain cybersecurity standards are already effective, however, and government agencies are becoming more active in enforcement. To be sure, many specific requirements, procedures and details are still waiting to be developed. Nonetheless, companies are proceeding to implement internal compliance programmes for cybersecurity and the protection of personal information. Under the existing Cybersecurity Law of China, companies are well advised to consider how and whether their existing business operations and practices warrant modification to ensure the requisite level of cybersecurity protection.

In Russia, the requirements for data localisation remain an important concern for international businesses. All personal data of Russian citizens must be stored and processed in the territory of Russia, and the location of such databases must be reported to the Russian data protection authority. Greater stringency of enforcement and more litigation are expected in the years ahead. The ‘Yarovaya Law’ also continues to pose concerns for telecom and internet companies. They are now required to store the contents of telephone calls and text messages for six months, and metadata for one year, and they must also provide significant additional assistance for government access and surveillance.

On 5 February 2018, the Asia Pacific Economic Cooperation (APEC) data protection framework saw Singapore join the United States (2012), Mexico (2013), Japan (2014), Canada (2015), and South Korea (2017) as an approved APEC economy participating in the APEC Cross-Border Privacy Rules system. APEC continues to grow slowly as countries and companies wait to see what develops.

Japan and the European Union announced on 17 July 2018 that they had agreed to grant reciprocal adequacy to their respective data protection regimes. To achieve this mutual recognition, the European Union had established certain conditions, including that Japan agree to treat trade union membership and sexual orientation as sensitive information categories; that data subject rights be accorded to information deleted within six months; and that original purpose limitations be respected; that Japan ensure that EU data transferred out of Japan to non-EU countries retain the same level of protection outside of Japan as in Japan. Also of note in Japan is a pending judicial ruling regarding a data breach case (Benesse Corporation). The decision here may define the obligations of businesses to protect personal information and the resulting damages from data breaches.

In addition to joining APEC, Singapore passed the Cybersecurity Act, which is primarily a criminal statute. However, it also created a new Commissioner of Cybersecurity with significant powers to prevent and respond to cybersecurity incidents. It also set up a licensing scheme for providers of certain cybersecurity services. As yet, no regulations or guidance have been provided for general business cybersecurity practices.
Canada finalised regulations to provide additional detail regarding the privacy breach notification requirement under the federal Personal Information Protection and Electronic Documents Act (PIPEDA). From 1 November 2018, private companies subject to PIPEDA will be required to notify affected individuals and report to the Privacy Commissioner where a breach of security safeguards would result in a real risk of significant harm to individuals. In 2018, the Federal Court of Canada also affirmed that PIPEDA applies to commercial entities outside Canada if they process personal information about Canadians. Privacy-related litigation in Canada is also expected to grow in the near term.

In Mexico, a significant cyberattack on financial institutions in 2018 is being investigated by the Attorney General. The national data protection authority (INAI) is also investigating to determine whether this incident constitutes a data breach. In addition, INAI has provided non-binding guidance on the status of biometric data as sensitive when (1) it refers to the most intimate sphere of the data subject, (2) can lead to discrimination, and (3) illegitimate use could result in material risk to the data subject. INAI also provided non-binding guidance for protecting personal data on social media.

In July 2018, Brazil adopted a comprehensive data protection law, known as the LGPD. This omnibus privacy regime is modelled closely on the GDPR. The LGPD also established a National Data Protection Authority. Significantly, an important case is pending before the Supreme Court regarding the legality of encryption technology. The issue concerns the role of encryption technology in preventing disclosure of communications content to law enforcement.

And, of course, much privacy and cybersecurity policymaking activity is taking place around the rest of the world as well.

* * *

The outline above highlights the in-depth treatment of the different jurisdictions discussed in detail below. As noted at the outset, 2018 may prove to be a turning point in global privacy and data protection policymaking. ‘Cambridge Analytica’ – shorthand for the active measures of Russia, and perhaps other geopolitical actors, to manipulate social media to interfere with the political processes of Western democracies – will likely become rallying cry for advocates on a par with the ‘Snowden’ impact on the privacy community in 2013.

In order to ensure that policymakers do not learn the wrong lessons from these dramatic events, it will be important for governments to focus precisely on combating real rather than imagined (or negligible) privacy risks. Such calculations are essential to achieve smart regulation rather than foolish over-regulation.

While privacy is, naturally, a fundamental right in democratic countries, governments must nonetheless justify their privacy regulations to their citizens. Without such rigorous justification, which entails a careful balancing of fundamental rights and other important social objectives, data protection policy could end up not actually being beneficial to society. Bad policy will delay or even deny technological development and deployment, thereby stunting social advancement and restricting consumer choice and economic options. ‘Artificial intelligence’ applications are likely to become the next proving ground for how smart regulators are. In all, however, the nurturing and preservation of human dignity and liberty will remain essential – of course.
I OVERVIEW

In the EU, data protection is principally governed by the EU General Data Protection Regulation (GDPR), which came into force on 25 May 2018 and is applicable in all EU Member States. The GDPR repeals the Data Protection Directive 95/46/EC, regulates the collection and processing of personal data across all sectors of the EU economy and introduces new data protection obligations for data controllers and processors alongside new rights for EU individuals.

The GDPR has created a single EU-wide law on data protection and has empowered Member State data supervisory authorities (DSAs) with significant enforcement powers, including the power to impose fines of up to 4 per cent of annual worldwide turnover or €20 million, whichever is greater, on organisations for failure to comply with the data protection obligations contained in the GDPR.

Set out in this chapter is a summary of the main provisions of the GDPR. We then cover guidance provided by the EU’s Article 29 Working Party (which has, since 25 May 2018, been replaced by the European Data Protection Board (EDPB)) on the topical issues of cloud computing and whistle-blowing hotlines. We conclude by considering the EU’s Network and Information Security Directive (the NIS Directive).

II THE GDPR

The GDPR imposes a number of obligations on organisations processing the personal data of individuals in the EU (data subjects). The GDPR also provides several rights to data subjects in relation to the processing of their personal data.

Failure to comply with the GDPR and Member State data protection laws enacted to supplement the data protection requirements of the GDPR can amount to a criminal offence and can result in significant fines and civil claims from data subjects who have suffered as a result.

1 William RM Long and Alan Charles Raul are partners, Géraldine Scali is a counsel and Francesca Blythe is an associate at Sidley Austin LLP.
Although the GDPR sets out harmonised data protection standards and principles, the 
GDPR grants EU Member States the power to maintain or introduce national provisions to 
further specify the application of the GDPR in Member State law.

i The scope of the GDPR

The GDPR applies to the processing of personal data wholly or partly by automated means 
and to the processing of personal data that forms part of a filing system or is intended to form 
part of a filing system other than by automated means. The GDPR does not apply to the 
processing of personal data by an individual in the course of a purely personal or household 
activity.

The GDPR only applies when the processing is carried out in the context of an 
establishment of the controller or processor in the European Union, or, where the controller 
or processor does not have an establishment in the European Union, but processes personal 
data in relation to the offering of goods or services to individuals in the European Union; 
or the monitoring of the behaviour of individuals in the European Union as far as their 
behaviour takes place within the European Union.

This means that many non-EU companies that have EU customers will need to comply 
with the data protection requirements in the GDPR.4

There are a number of important terms used in the GDPR,5 including:

a controller: any natural or legal person who alone or jointly with others, determines the 
purpose and means of processing personal data;
b data processor: a natural or legal person who processes personal data on behalf of the 
controller;
c data subject: an identified or identifiable individual who is the subject of the personal 
data;
d establishment: the effective and real exercise of activity through stable arrangements in 
a Member State;6
e filing system: any structured set of personal data that is accessible according to specific 
criteria, whether centralised or decentralised or dispersed on a functional or geographical 
basis, such as a filing cabinet containing employee files organised according to their 
date of joining or their names or location;
f personal data: any information that relates to an identified or identifiable individual 
who can be identified, directly or indirectly, by reference to an identifier such as a name, 
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 individual. In practice, this is a broad definition including anything 
from someone’s name, address or national insurance number to information about 
their taste in clothes. Additionally, personal data that has undergone pseudonymisation, 
where the personal data has been through a process of de-identification so that a coded 
reference or pseudonym is attached to a record to allow the data to be associated to a 
particular data subject without the data subject being identified, is personal data under 
the GDPR; and

4 Article 3(1) of the GDPR.
5 Article 4 of the GDPR.
6 Recital 22 of the GDPR.
processing: any operation or set of operations performed upon 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. This definition is so broad that it covers practically any activity in relation to personal data.

ii Obligations and processors of controllers under the GDPR

Notification
The notification obligation under the Data Protection Directive requiring controllers to notify their national data supervisory authority prior to carrying out any processing of personal data no longer exists under the GDPR. Instead, DSAs may introduce their own notification requirements. For example, the UK’s data supervisory authority, the Information Commissioners Office (ICO), requires controllers to register on a public register maintained by the ICO, in addition to paying a fee to the ICO ranging from £40 to £2,400 depending on the type of organisation the controller is.

Importantly, instead of the notification obligation, Article 30 of the GDPR requires controllers to maintain a record of their processing, which should include the purpose of the processing; a description of the categories of data subjects and of the categories of personal data; the categories of recipients to whom the personal data has been or will be disclosed including recipients in third countries (non-EEA Member States); identifying the third country if there are transfers of personal data to a third country; envisaged time limits for the erasure of the different categories of personal data; and a general description of the technical and organisational security measures in place to protect the personal data.

Data protection principles and accountability
Generally, the GDPR requires controllers to comply with the following data protection principles when processing personal data:

a the lawfulness, fairness and transparency principle: personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject;

b the purpose limitation principle: personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

c data minimisation principle: personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d accuracy principle: personal data must be accurate and, where necessary, kept up to date, and every reasonable step must be taken to ensure that personal data that are inaccurate in relation to the purposes for which they are processed are erased or rectified without delay;

7 Article 5(1)(a) of the GDPR.
8 Article 5(1)(b) of the GDPR.
9 Article 5(1)(c) of the GDPR.
10 Article 5(1)(d) of the GDPR.
storage limitation principle: 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;

integrity and confidentiality: personal data must be processed in a manner that ensures appropriate security of personal data as described below; and

accountability: the GDPR’s principle of accountability under Article 5(2) of the GDPR is a central focus of the data protection requirements in the GDPR and requires controllers to process personal data in accordance with data protection principles found in the GDPR. Article 24 of the GDPR further provides that controllers implement appropriate technical and organisational measures to ensure and to be able to demonstrate that data processing is performed in accordance with the GDPR.

Data protection impact assessments (DPIA)

Article 35(1) of the GDPR imposes an obligation on controllers to conduct a DPIA prior to the processing of personal data, where the processing is likely to result in a high risk to the rights and freedoms of data subjects. This may be relevant to certain activities of the controller such as where it decides to carry out extensive monitoring of its employees. The controller is required to carry out a DPIA, which assesses the impact of the envisaged processing on the personal data of the data subject, taking into account the nature, scope, context and purposes of the processing.

Article 35(3) of the GDPR provides that a DPIA must be conducted where the controller engages in:

a a systematic and extensive evaluation of personal aspects relating to data subjects which is based on automated processing, including profiling, and produces legal effects concerning the data subject or similarly significantly affecting the data subject; or

b processing on a large scale special categories of personal data under Article 9(1) of the GDPR, or of personal data revealing criminal convictions and offences under Article 10 of the GDPR; or

c a systematic monitoring of a publicly accessible area on a large scale.

In addition, organisations must carry out a DPIA when using new technologies; and where the processing is likely to result in a high risk to the rights and freedoms of data subjects.

Article 35(4) of the GDPR requires the DSA to publish a list of activities in relation to which a DPIA should be carried out. If the controller has appointed a Data Protection Officer (DPO), the controller should seek the advice of the DPO when carrying out the DPIA.

Importantly, Article 36(1) of the GDPR states that where the outcome of the DPIA indicates that the processing involves a high risk, which cannot be mitigated by the controller, the DSA should be consulted prior to the commencement of the processing.

A DPIA involves balancing the interests of the controller against those of the data subject. Article 35(7) of the GDPR states that a DPIA should contain at a minimum:

a a description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the controller;

b an assessment of the necessity and proportionality of the processing operations in relation to the purpose of the processing;

---

11 Article 5(1)(e) of the GDPR.
c an assessment of the risks to data subjects; and
d the measures in place to address risk, including security and to demonstrate compliance with the GDPR, taking into account the rights and legitimate interests of the data subject.

The Article 29 Working Party (WP29) noted in its guidelines on DPIAs that the reference to the ‘rights and freedoms’ of data subjects under Article 35 of the GDPR while primarily concerned with rights to data protection and privacy also includes other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition on discrimination, right to liberty and conscience and religion.12

The WP29 introduced the following nine criteria that should be considered by controllers when assessing whether their processing operations require a DPIA, owing to their inherent high risk13 to data subjects rights and freedoms:

a evaluation or scoring, including profiling and predicting, especially from ‘aspects concerning the data subject’s performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements’;
b automated-decision making with legal or similar significant effects – processing that aims at taking decisions on data subjects producing ‘legal effects concerning the natural person’ or which ‘similarly significantly affects the natural person’. For example, the processing may lead to the exclusion or discrimination against data subjects. Processing with little or no effect on data subjects does not match this specific criterion;
c systematic monitoring – processing used to observe, monitor or control data subjects, including data collected through networks or ‘a systematic monitoring of a publicly accessible area’. This type of monitoring is a criterion because the personal data may be collected in circumstances where data subjects may not be aware of who is collecting their data and how their data will be used;
d sensitive data or data of a highly personal nature – this includes special categories of personal data as defined in Article 9 of the GDPR (for example information about individuals’ political opinions), as well as personal data relating to criminal convictions or offences as defined in Article 10 of the GDPR. An example would be a hospital keeping patients’ medical records or a private investigator keeping offenders’ details. Additionally, beyond the GDPR, there are some categories of data that can be considered as increasing the possible risk to the rights and freedoms of data subjects. These personal data are considered as sensitive (as the term is commonly understood) because they are linked to household and private activities (such as electronic communications whose confidentiality should be protected), or because they impact the exercise of a fundamental right (such as location data whose collection questions the freedom of movement) or because their violation clearly involves serious impacts in the data subject’s daily life (such as financial data that might be used for payment fraud);

---

12 Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is ‘likely to result in a high risk’ for the purposes of Regulation 2016/679, WP 248, as last revised and adopted on 4 October 2017, page 6.

13 Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is ‘likely to result in a high risk’ for the purposes of Regulation 2016/679, WP 248, as last revised and adopted on 4 October 2017, pages 9–11.
data processed on a large scale: the GDPR does not define what constitutes large-scale. In any event, the WP29 recommends that the following factors, in particular, be considered when determining whether the processing is carried out on a large scale:

- the number of data subjects concerned, either as a specific number or as a proportion of the relevant population;
- the volume of data and/or the range of different data items being processed;
- the duration, or permanence, of the data processing activity; and
- the geographical extent of the processing activity.

Matching or combining datasets, for example originating from two or more data processing operations performed for different purposes or by different controllers in a way that would exceed the reasonable expectations of the data subject;

data concerning vulnerable data subjects – the processing of this type of data is a criterion because of the increased power imbalance between the data subjects and the data controller, meaning the data subjects may be unable to easily consent to, or oppose, the processing of their data, or exercise their rights. Vulnerable data subjects may include children as they can be considered as not able to knowingly and thoughtfully oppose or consent to the processing of their data and employees; and

Innovative use or applying new technological or organisational solutions, for example, combining use of finger print and face recognition for improved physical access control. The GDPR makes it clear that the use of a new technology, defined in ‘accordance with the achieved state of technological knowledge’ can trigger the need to carry out a DPIA. This is because the use of such technology can involve novel forms of data collection and usage, possibly with a high risk to data subjects’ rights and freedoms. Furthermore, the personal and social consequences of the deployment of a new technology may be unknown.

When the processing in itself ‘prevents data subjects from exercising a right or using a service or a contract’. This includes processing operations that aim to allow, modify or refuse data subjects’ access to a service or entry into a contract. An example of this is where a bank screens its customers against a credit reference database in order to decide whether to offer them a loan.

Additionally, the WP29 noted that the mere fact the controller’s obligation to conduct a DPIA has not been met does not negate its general obligation to implement measures to appropriately manage risks to the rights and freedoms of the data subject when processing their personal data.\(^{14}\) In practice, this means controllers are required to continuously assess the risks created by their processing activities in order to identify when a type of processing is likely to result in a high risk to the rights and freedoms of the data subject.

The WP29 recommend that as a matter of good practice, controllers should continuously review and regularly reassess their DPIAs.\(^{15}\)

---

\(^{14}\) Article 29 Data Protection Working Party Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is ‘likely to result in a high risk’ for the purposes of Regulation 2016/679, WP 248, as last revised and adopted on 4 October 2017, page 6.

\(^{15}\) Article 29 Data Protection Working Party Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is ‘likely to result in a high risk’ for the purposes of Regulation 2016/679, WP 248, as last revised and adopted on 4 October 2017, page 14.
**Data protection by design and by default**

Article 25 of the GDPR requires controllers to, at the time of determining the means of processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation and anonymisation, which are designed to implement the data protection principles in the GDPR, in an effective manner, and to integrate the necessary and appropriate safeguards into the processing of personal data in order to meet the data protection requirements of the GDPR and protect the rights of the data subject.

Controllers are also under an obligation to implement appropriate technical and organisational measures that ensure that, by default, only personal data necessary for each specific purpose of the processing are processed. This obligation under Article 25(2) of the GDPR covers the amount of personal data collected, the extent of the processing of the personal data, the period of storage of the personal data and its accessibility.

**DPOs**

Article 37 of the GDPR requires both controllers and processors to appoint DPOs where:

a) the processing is carried out by a public authority or body, except where courts are acting in their judicial capacity;

b) the core activities of the controller or processor consist of processing operations that, by virtue of their nature, scope or purpose, require regular and systematic monitoring of data subjects on a large scale; or

c) the core activities of the controller or processor consist of processing on a large scale special categories of personal data pursuant to Article 9 of the GDPR or personal data about criminal convictions and offences pursuant to Article 10 of the GDPR.

The WP29, in its guidance on DPOs, note that ‘core activities’ can be considered key operations\(^{16}\) required to achieve the controller or processor’s objectives. However, it should not be interpreted as excluding the activities where the processing of personal data forms an ‘inextricable’ part of the controller or processor’s activities. The WP29 provides the example of the core activity of a hospital being to provide healthcare. However, it cannot provide healthcare effectively or safely without processing health data, such as patients’ records.\(^{17}\)

Any DPO appointed must be appointed on the basis of their professional qualities and expert knowledge of data protection law and practices.\(^{18}\) The WP29 note personal qualities of the DPO should include integrity and high professional ethics, with the DPO’s primary concern being enabling compliance with the GDPR.\(^{19}\)

Staff members of the controller or processor may be appointed as a DPO, as can a third-party consultant. Once the DPO has been appointed, the controller or processor must provide their contact details to their DSA.\(^{20}\)

---

\(^{16}\) Article 29 Working Party, Guidelines on Data Protection Officers (‘DPOs’), WP 243, as last revised and adopted on 5 April 2017, page 20.

\(^{17}\) Article 29 Working Party Guidelines on Data Protection Officers (‘DPOs’), WP 243, as last revised and adopted on 5 April 2017, page 7.

\(^{18}\) Article 37(5) of the GDPR.

\(^{19}\) Article 37(7) of the GDPR.

\(^{20}\) Article 37(7) of the GDPR.
A DPO must be independent, whether or not he or she is an employee of the respective controller or processor and must be able to perform his or her duties in an independent manner. The DPO can hold another position but must be free from a conflict of interests. For example, the DPO could not hold a position within the controller organisation that determined the purposes and means of data processing, such as the head of marketing, IT or human resources.

Once appointed, the DPO is expected to perform the following, non-exhaustive list of tasks.

a inform and advise the controller or processor and the employees who carry out the processing of the GDPR obligations and relevant Member State data protection obligations;

b monitor compliance with the GDPR, and other relevant Member State data protection obligations, and oversee the data protection 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 the processing operations and the related audits;

c provide advice where requested in relation to the DPIA;

d cooperate with the DSA; and

e act as the contact point for the DSA on issues relating to processing.

The GDPR also provides the option, where controllers or processors do not meet the processing requirements necessary to appoint a DPO, to voluntarily appoint one. The WP29 recommends in its guidance on DPOs that even where controllers or processors come to the conclusion that a DPO is not required to be appointed, the internal analysis carried out to determine whether or not a DPO should be appointed should be documented to demonstrate that the relevant factors have been taken into account properly.

Lawful grounds for processing
Controllers may only process personal data if they have satisfied one of six conditions:

a the data subject in question has consented to the processing;

b the processing is necessary to enter into or perform a contract with the data subject;

c the processing is necessary for the purposes of the legitimate interests pursued by the controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject that require protection of the personal data;

d the processing is necessary to comply with a legal obligation to which the controller is subject;

e the processing is necessary to protect the vital interests of the data subject; or

f the 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. Of these conditions, the first three will be most relevant to business.

21 Recital 97 of the GDPR.
22 Article 39 of the GDPR.
23 Article 37(4) of the GDPR.
24 Article 29 Working Party Guidelines on Data Protection Officers (DPOs), WP 243, as last revised and adopted on 5 April 2017, page 5.
25 Article 6 of the GDPR.
Personal data that relates to a data subject’s racial or ethnic origin, political opinions, trade union membership, religious or philosophical beliefs, 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 (sensitive personal data) can only be processed in more narrowly defined circumstances.26 The circumstances that are often be most relevant to a business are where the data subject has explicitly consented to the processing or the processing is necessary for the purposes of carrying out its obligations in the field of employment and social security and social protection law.

The WP29 state in its guidance on consent, that where controllers intend to rely on consent as a lawful processing ground, they have a duty to assess whether they will meet all of the GDPR requirements to obtain valid consent.27 Valid consent under the GDPR is a clear affirmative act that should be freely given, specific, informed and an unambiguous indication of the data subject's agreement to the processing of their personal data. Consent is not regarded as freely given where the data subject has no genuine or free choice or is not able to refuse or withdraw consent without facing negative consequences. For example, where the controller is in a position of power over the data subject, such as an employer, the employee's consent is unlikely to be considered freely given or a genuine or free choice, as to choose to withdraw consent or refuse to give initial consent in the first place could result in the employee facing consequences detrimental to their employment.

As the WP29 notes, consent can only be an appropriate lawful basis for processing personal data if the data subject is offered control and a genuine choice with regard to accepting or declining the terms offered or declining them without negative effects.28 Without such genuine and free choice, the WP29 notes the data subject's consent becomes illusory and consent will be invalid, rendering the processing unlawful.29

**Provision of information**

Certain information needs to be provided by controllers to data subjects when controllers collect personal data about them, unless the data subjects already have that information. Article 13 of the GDPR provides a detailed list of the information required to be provided to data subjects either at the time the personal data is obtained or immediately thereafter, including:

- the identity and contact details of the controller (or the controller’s representative);
- the contact details of the DPO, where applicable;
- the purposes of the processing;
- the legal basis for the processing;
- the recipients or categories of recipients of the personal data;
- where the personal data is intended to be transferred to a third country, reference to the appropriate legal safeguard to lawfully transfer the personal data;
- the period for which the personal data will be stored or where that is not possible, the criteria used to determine that period;

---

26 Article 9 of the GDPR.
28 ibid.
29 ibid.
the existence of rights of data subjects to access, correct, restrict and object to the processing of their personal data;

the right to lodge a complaint with a DSA; and

whether the provision of personal data is a statutory or contractual requirement or a requirement necessary to enter into a contract.

In instances where the personal data are not collected by the controller directly from the data subject concerned, the controller is expected to provide the above information to the data subject, in addition to specifying the source of the personal data, within a reasonable time period after obtaining the personal data, but no later than a month after having received the personal data or if the personal data is to be used for communication with the data subject, at the latest, at the time of the first communication to that data subject.\(^{30}\) In cases of indirect collection, it may also be possible to avoid providing the required information if to do so would be impossible or involve a disproportionate effort, or if the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law or obtaining or disclosure of personal data is expressly laid down by Union or Member State law to which the controller is subject.\(^ {31}\)

The WP29 notes that in order to ensure the information notices are concise, transparent, intelligible and easily accessible under Article 12 of the GDPR, controllers should present the information efficiently and succinctly to prevent the data subjects from experiencing information fatigue.\(^ {32}\)

iii Security and breach reporting

The GDPR requires controllers and, where applicable, processors to ensure that appropriate technical and organisational measures are in place to protect personal data and ensure a level of security appropriate to the risk.\(^ {33}\) Such technical and organisational measures include the pseudonymisation of personal data, encryption of personal data, anonymisation of personal data, and de-identification of personal data, which occurs where the information collected has undergone a process that involves the removal or alteration of personal identifiers and any additional techniques or controls required to remove, obscure, aggregate or alter the information in such a way that no longer identifies the data subject. Additionally, controllers must also ensure that when choosing a data processor they choose one that provides sufficient guarantees as to the security measures applied when processing personal data on behalf of the controller, pursuant to Article 28 of the GDPR. A controller must also ensure that it has in place a written contract with the data processor under which the data processor undertakes to comply with data protection requirements under Article 28 of the GDPR, including only processing the personal data on the instructions of the controller and being subject to the same data protection obligations as set out in the contract between the controller and

---

\(^{30}\) Article 14(3) of the GDPR.

\(^{31}\) Article 14(5) of the GDPR.

\(^{32}\) Article 29 Working Party Guidelines on transparency under Regulation 2016/679, as last revised and adopted on 11 April 2018, page 7.

\(^{33}\) Article 32 of the GDPR.
processor. Under such an agreement, the processor will remain liable for the failure of the sub-processor to perform its data protection obligations under the agreement between the processor and the sub-processor.34

**Personal data breaches**

Article 4(1) of the GDPR defines a personal data breach broadly as a ‘breach of security leading to the accidental or unlawful destruction, loss, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed’. According to the guidelines published by the WP29 on personal data breach notification under the GDPR35 personal data breaches typically fall in one of the following categories:

- **a** confidentiality breaches: where there is an unauthorised or accidental disclosure of, or access to, personal data;
- **b** availability breaches: where there is an accidental or unauthorised loss of access to, or destruction of, personal data; and
- **c** integrity breaches: where there is an unauthorised or accidental alteration of personal data.

Additionally, controllers are required, with the assistance of the processors, where applicable, to report personal security breaches that are likely to result in a risk to the rights and freedoms of the data subject, to the relevant DSA without undue delay and, where feasible, not later than 72 hours after having first become aware of the personal data breach. Where the processor becomes aware of a personal data breach it is under an obligation to report the breach to the controller. Upon receiving notice of the breach from the processor, the controller is then considered aware of the personal data breach and has 72 hours to report the breach to the relevant DSA.

The WP29 note in its guidance on personal data breaches that the controller should have internal processes in place that are able to detect and address a personal data breach.36 The WP29 provide the example of using certain technical measures such as data flow and log analysers to detect any irregularities in processing of personal data by the controller.37 Importantly, the WP29 note that once a breach is detected it should be reported upwards to the appropriate level of management so it can be addressed and contained effectively. These measures and reporting mechanisms could, in the view of the WP29, be set out in the controller’s incident response plans.38

**Exceptions**

Controllers are exempted from notifying a personal data breach to the relevant DSA if it is able to demonstrate that the personal data breach is unlikely to result in a risk to the rights and freedoms of data subjects. In assessing the level of risk, the following factors should be taken into consideration:

34 Article 28(4) of the GDPR.
37 ibid.
38 ibid.
Type of personal data breach: is it a confidentiality, availability, or integrity type of breach?

Nature, sensitivity and volume of personal data: usually, the more sensitive the data, the higher the risk of harm from a data subject’s point of view. Also, combinations of personal data are typically more sensitive than single data elements.

Ease of identification of data subjects: the risk of identification may be low if the data were protected by an appropriate level of encryption. In addition, pseudonymisation can reduce the likelihood of data subjects being identified in the event of a breach.

 Severity of consequences of data subjects: especially if sensitive personal data are involved in a breach, the potential damage to data subjects can be severe and thus the risk may be higher.

Special characteristics of the data subjects: data subjects who are in a particularly vulnerable position (e.g., children) are potentially at greater risk if their personal data are breached.

Number of affected data subjects: generally speaking, the more data subjects that are affected by a breach, the greater the potential impact.

Special characteristics of the controller: for example, if a breach involves controllers who are entrusted with the processing of sensitive personal data (e.g., health data), the threat is presumed to be greater.

Other general considerations: assessing the risk associated with a breach can be far from straightforward. Therefore the WP29, in its guidance on personal data breach notifications, refers to the recommendations published by the European Union Agency for Network and Information Security (ENISA), which provides a methodology for assessing the severity of the breach and which may help with designing breach management response plans.

Notifying affected data subjects

In addition to notifying the relevant DSA, in certain cases controllers may also be required to communicate the personal data breach to affected data subjects (i.e. when the personal data breach is likely to result in a ‘high risk’ to the rights and freedoms of data subjects). The specific reference in the law to high risk indicates that the threshold for communicating a breach to data subjects is higher than for notifying the DSAs – taking account of the risk factors listed above.

It should be noted that the accountability requirements in the GDPR summarised above, such as purpose limitation, data minimisation and storage limitation, mean, for example, that implementing technical controls in isolation, or the piecemeal adoption of data security standards, are unlikely to be sufficient to ensure compliance. As a default position, controllers should seek to minimise the collection and retention of personal data, and especially where sensitive personal data are collected and retained, ensure that those data are encrypted or otherwise made unintelligible to unauthorised parties, to the greatest extent possible.

iv Prohibition on transfers of personal data outside the EEA

Controllers may not transfer personal data to countries outside of the European Economic Area (EEA) unless the recipient country provides an adequate level of protection for the personal data. The European Commission can make a finding on the adequacy of any particular non-EEA state and Member States are expected to give effect to these findings as necessary in their national laws. So far, the European Commission has made findings of adequacy with respect to Andorra, Argentina, Canada, the Faroe Islands, Guernsey, the Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay. On 17 July 2018, the European Commission and Japan reached a mutual adequacy agreement, which included the Commission finding Japan has a level of protection of personal data comparable to that of the EU, and is therefore considered adequate. In addition, the United States previously reached agreement with the European Commission on a set of ‘Safe Harbor’ principles to which organisations in the United States could subscribe to be deemed ‘adequate’ to receive personal data from controllers in the EU. However, in October 2015 this was declared invalid by the Court of Justice of the European Union (CJEU), leading to intense negotiations between US authorities and the European Commission to develop a replacement trans-Atlantic data transfer mechanism. Then, on 12 July 2016, the Privacy Shield was adopted by the European Commission, with US companies being able to self-certify under the Privacy Shield from 1 August 2016 in order to receive personal data from controllers in the EU. On 11 June 2018, European members of the European Parliament’s Committee on Civil Liberties, Justice and Home Affairs (MEPs), voted in favour of the suspension of the Privacy Shield until the US is in full compliance with the data protection requirements contained in the Privacy Shield. In July 2018, the European Parliament adopted the resolution and called on the US to comply with the requirements of the Privacy Shield, such as the appointment of an ombudsman to deal with complaints by data subjects in relation to the Privacy Shield and to remove organisations who fail to comply with data protection requirements from the Privacy Shield. The Privacy Shield is due for its second annual review by the European Commission in October 2018. The European Commission has unilateral powers to revoke the Privacy Shield where it no longer considers the Privacy Shield is able to effectively protect the personal data of EU citizens when transferred to the US.

Where transfers are to be made to countries that are not deemed adequate, other exceptions may apply to permit the transfer. The European Commission has approved EU model contract clauses, standard contractual clauses that may be used by controllers and processors when transferring personal data from the EU to non-EEA countries (a model contract). There are two forms of model contract: one where both the data exporter and data importer are controllers; and another where the data exporter is a controller and the data importer is a data processor. Personal data transferred on the basis of a model contract will be

---

40 The EEA consists of the 28 EU Member States together with Iceland, Liechtenstein and Norway.
41 Article 45 of the GDPR.
42 The US–EU Safe Harbor Framework was approved in 2000. Details of the Safe Harbor Agreement between the EU and the United States can be found in European Commission Decision 520/2000/EC.
43 Judgment of the Court (Grand Chamber) of 6 October 2015 – Maximillian Schrems v. Data Protection Commissioner.
45 Article 46 of the GDPR.
46 Article 46(2)(c) of the GDPR.
presumed to be adequately protected. However, model contracts have been widely criticised as being onerous on the parties. This is because they grant third-party rights to data subjects to enforce the terms of the model contract against the data exporter and data importer, and require the parties to the model contract to give broad warranties and indemnities. The clauses of the model contracts also cannot be varied and model contracts can become impractical where a large number of data transfers need to be covered by numerous model contracts. However, the status of model contracts is currently uncertain, as following questions as to the validity of model contracts from the Irish Data Protection Commissioner, the Irish High Court has referred the questions to the CJEU for a preliminary ruling to determine the legal status of model contracts.

An alternative means of authorising transfers of personal data outside the EEA is the use of binding corporate rules. This approach may be suitable for multinational companies transferring personal data within the same company, or within a group of companies. Under the binding corporate rules approach, the company would adopt a group-wide data protection policy that satisfies certain criteria and, if the rules bind the whole group, then those rules could be approved by the relevant DSA as providing adequate data protection for transfers of personal data throughout the group. The WP29 have published various documents on binding corporate rules, including a model checklist for the approval of binding corporate rules, a table setting out the elements and principles to be found in binding corporate rules and recommendations on the standard application for approval of controller and processor binding corporate rules.

In addition to binding corporate rules and other data transfer solutions, the transfer of personal data outside of the EEA can occur via the use of approved codes of conduct or certification mechanisms.

v Rights of the data subject
The GDPR provides for a series of rights data subjects can use in relation to the processing of their personal data, with such rights subject to certain restrictions or limitations.

---

WP 195 – Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules adopted on 6 June 2012.
WP 195a – Recommendation 1/2012 on the standard application form for approval of Binding Corporate Rules for the transfer of personal data for processing activities adopted on 17 September 2012.
WP 153 – Working Document setting up a table with the elements and principles to be found in binding corporate rules adopted on 24 June 2008.
49 WP 264 – Recommendation on the Standard Application form for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data – Adopted on 11 April 2018.

© 2018 Law Business Research Ltd
Timing and costs
The GDPR requires that a data subject’s rights request be complied with without undue delay and in any event within one month of receipt of the request. If the request is particularly complex, then this period can be extended to three months if the data subject is informed of the reasons for the delay within one month. Where it is determined that compliance with the request is not required, then data subjects should be informed of this within one month together with the reasons as to why the request is not being complied with and the fact that they can lodge a complaint with a DSA and seek a judicial remedy.

A fee must not be charged for compliance with a data subject’s rights request unless it can be demonstrated that the request is manifestly unfounded or excessive.

Right to access personal data
Article 15 of the GDPR provides data subjects with the right to access their personal data processed by the controller. The right requires controllers to confirm whether or not they are processing the data subject’s personal data and confirm:

a. the purpose of the processing;
b. the categories of personal data concerned;
c. the recipients or categories of recipients to whom the personal data has been or will be disclosed to, in particular recipients in third countries;
d. where possible, the retention period for storing the personal data, or, where that is not possible, the criteria used to determine that period;
e. the existence of the right to request from the controller rectification, erasure, restriction or objection to the processing of their personal data;
f. the right to lodge a complaint with the DSA;
g. where personal data is not collected from the data subject, the source of the personal data; and
h. the existence of automated decision making, including profiling, where applicable.

Under the right of access to personal data, the controller is required to provide a copy of the personal data undergoing processing.

This right is not absolute, but subject to a number of limitations, including the right to obtain a copy of the personal data shall not adversely affect the rights and freedoms of others.51 According to Recital 63 of the GDPR, these rights may include trade secrets or other intellectual property rights. As such, before disclosing information in response to a subject access request, controllers should first consider whether the disclosure would adversely affect the rights of any third party’s personal data; and the rights of the controller and in particular, its intellectual property rights. However, even where such an adverse effect is anticipated, the controller cannot simply refuse to comply with the access request. Instead, the controller would need to take steps to remove or redact information that could impact the rights or freedoms of others.

Where the controller processes a large quantity of the data subject’s personal data, as would likely be the case in respect of an organisation and its employees, the controller has a right to request that, before the personal data is delivered, the data subject should specify the

51 Article 15(4) of the GDPR.
information or processing activities to which the request relates. However, caution should be exercised when requesting further information from the data subject as it is likely that under the GDPR a controller will not be permitted to narrow the scope of a request itself.

Where the controller is able to demonstrate that the data subject’s request for access to the personal data the controller holds is manifestly unfounded or excessive because of its repetitive nature, the controller can refuse to comply with the data subject’s request. However, in the absence of guidance or case law to provide parameters around the scope of these exemptions, a strict interpretation should be considered for the concept of ‘manifestly unfounded’ with repetitive requests being documented in order to fulfil the burden of proof as to their excessive character.

If the controller has reasonable doubts concerning the identity of the data subject making the access request, the controller can request the provision of additional information necessary to confirm the identity of the data subject.

If the controller is able to demonstrate that it is not in a position to identify the data subject, it can refuse to comply with a data subject’s request to access their personal data.

**Right of rectification of personal data**

Article 16 of the GDPR provides data subjects with the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her.

The right is not absolute but subject to certain limitations or restrictions, including:

- where the controller is able to demonstrate that the data subject’s request for rectification of their personal data the controller holds is manifestly unfounded or excessive because of its repetitive nature, the controller can refuse to comply with the data subject’s request;
- where the controller has reasonable doubts concerning the identity of the data subject making the request, the controller can request the provision of additional information necessary to confirm the identity of the data subject; and
- where the controller is able to demonstrate that it is not in a position to identify the data subject, it can refuse to comply with a data subject’s request to access their personal data.

**Right of erasure of personal data (‘right to be forgotten’)**

Article 17 of the GDPR provides data subjects with the right of erasure of their personal data the controller holds without undue delay, where:

- the personal data are no longer necessary for the purposes for which they were collected.

---

52 Recital 63 of the GDPR.
53 Article 12(5) of the GDPR.
54 Article 12(6) of the GDPR.
55 Article 12(2) of the GDPR.
56 Article 12(5) of the GDPR.
57 Article 12(6) of the GDPR.
58 Article 12(2) of the GDPR.
59 Article 17(1)(a) of the GDPR.
the data subject withdraws consent to the processing and there is no other legal ground for the processing;  
the data subject objects to the processing and there are no overriding legitimate grounds for the processing;  
the personal data has been unlawfully processed;  
the personal data has to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;  
the personal data has been collected in connection with an online service offered to a child.

However, the right of erasure is not absolute and is subject to certain restrictions or limitations:

- the data subject's right of erasure will not apply where the processing is necessary for exercising the right of freedom and expression and information;
- where complying with a legal obligation which requires processing by Union or Member State law;
- reasons of public interest in the area of public health in accordance with Article 9(2)(h) and (i);
- for archiving purposes in the public interest, scientific, historical research or statistical research purposes;
- for the establishment, exercise or defence of legal claims;
- where the controller is able to demonstrate that the data subject's request for rectification of their personal data the controller holds is manifestly unfounded or excessive because of its repetitive nature, the controller can refuse to comply with the data subject's request;
- where the controller has reasonable doubts concerning the identity of the data subject making the request, the controller can request the provision of additional information necessary to confirm the identity of the data subject; and
- where the controller is able to demonstrate that it is not in a position to identify the data subject, it can refuse to comply with a data subject's request to access their personal data.

**Right to restriction of processing**

Article 18 of the GDPR also provides data subjects with the right to restrict the processing of their personal data in certain circumstances. The restriction of processing means that, with the exception of storage, the personal data can only be processed where:

- the accuracy of the personal data is contested by the data subject, enabling the controller to verify the accuracy of the personal data;

---

60 Article 17(1)(b) of the GDPR.
61 Article 17(1)(c) of the GDPR.
62 Article 17(1)(d) of the GDPR.
63 Article 17(1)(e) of the GDPR.
64 Article 17(1)(f)) of the GDPR.
65 Article 12(5) of the GDPR.
66 Article 12(6) of the GDPR.
67 Article 12(2) of the GDPR.
68 Article 17(3) of the GDPR.
b the processing is unlawful and the data subject opposes the erasure of the personal data and requests restriction of the processing;

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 the processing pursuant to Article 21(1) of the GDPR, pending the verification of whether the legitimate grounds of the controller override those of the data subject.

The right of the data subject to request the restriction of the processing of their personal data is not absolute and is qualified:

a where the controller is able to demonstrate that the data subject’s request for rectification of their personal data the controller holds is manifestly unfounded or excessive because of its repetitive nature, the controller can refuse to comply with the data subject’s request;²⁶

b where the controller has reasonable doubts concerning the identity of the data subject making the request, the controller can request the provision of additional information necessary to confirm the identity of the data subject;²⁷ and

c where the controller is able to demonstrate that it is not in a position to identify the data subject, it can refuse to comply with a data subject’s request to access their personal data.²⁸

**Right to data portability**

Article 20 of the GDPR provides data subjects with the right to receive their personal data which they have provided to the controller, in a structured, commonly used and machine-readable format and have the right to transmit their personal data to another controller without hindrance, where the processing is based on consent pursuant to Article 6(1)(a) or 9(2)(a) of the GDPR; and where the processing is carried out by automatic means.

This right would, for example, permit a user to have a social media provider transfer his or her personal data to another social media provider.

Article 20(2) of the GDPR limits the requirement for a controller to transmit personal data to a third-party data controller where this is ‘technically feasible’. The WP29 have published guidance on the right to data portability, stating that a transmission to a third-party data controller is ‘technically feasible’ when ‘communication between two systems is possible, in a secured way, and when the receiving system is technically in a position to receive the incoming data’.²⁹

---

²⁶ Article 12(5) of the GDPR.
²⁷ Article 12(6) of the GDPR.
²⁸ Article 12(2) of the GDPR.
²⁹ Article 29 Working Party, Guidelines on the right to data portability, WP 242, adopted on 13 December 2016 (as last revised and adopted on 5 April 2017), page 16.
In addition, the WP29 guidance recommends that controllers begin developing technical tools to deal with data portability requests and that industry stakeholders and trade associations should collaborate to deliver a set of interoperable standards and formats to deliver the requirements of the right to data portability.73

The guidance also clarifies which types of personal data the right to data portability should apply to, specifically:

a) that the right applies to data provided by the data subject, whether knowingly and actively as well as the personal data generated by his or her activity;74

b) the right does not apply to data inferred or derived by the controller from the analysis of data provided by the data subject (e.g., a credit score);75 and

c) the right is not restricted to data communicated by the data subject directly.76

Right to object to the processing of personal data

Article 21 of the GDPR provides data subjects with the right to object to the processing of their personal data. This right includes the right to object to:

a) processing where the controller’s legal basis for the processing of the personal data is either necessary for public interest purposes or where the processing is in the legitimate interests of the controller (‘general right to object’);

b) processing for direct marketing purposes (the ‘right to object to marketing’); and

c) processing necessary for scientific or historical research purposes or statistical purposes and the data subject has grounds to object that relate to ‘his or her particular situation’.

The right of the data subject to object to the processing of their personal data is not absolute:

a) where the data subject can demonstrate compelling legitimate grounds for the processing which overrides the interests, rights and freedoms of the data subject or where the processing is necessary for the establishment, exercise or defence of legal claims;77 or

b) where the processing is necessary for research purposes, there is an exemption to the right of data subjects to object where the processing is necessary for the performance of a task carried out for reasons of public interest.78

73 Article 29 Working Party, Guidelines on the right to data portability, WP 242, adopted on 13 December 2016 (as last revised and adopted on 5 April 2017), page 3.
74 Article 29 Working Party, Guidelines on the right to data portability, WP 242, adopted on 13 December 2016 (as last revised and adopted on 5 April 2017), page 10.
75 Article 29 Working Party, Guidelines on the right to data portability, WP 242, adopted on 13 December 2016 (as last revised and adopted on 5 April 2017), page 10.
76 Article 29 Working Party, Guidelines on the right to data portability, WP 242, adopted on 13 December 2016 (as last revised and adopted on 5 April 2017), page 3.
77 Article 21(1) of the GDPR.
78 Article 21(6) of the GDPR.
vi Enforcement under the GDPR

DSAs, lead DSAs and ‘one-stop shop’

Enforcement of the GDPR is done at a national level through national or state DSAs. In addition, one of the aims of the GDPR was to enable a controller that processes personal data in different EU Member States to deal with one Lead DSA, known as the ‘One Stop Shop’ mechanism.

The one-stop shop mechanism

Under Article 56 of the GDPR, a controller or processor that carries out cross-border processing will be primarily regulated by a single lead DSA where the controller or processor has its main establishment.

Article 4(23) of the GDPR defines cross-border processing as either:

a processing of personal data that takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the EU where the controller or processor is established in more than one Member State (i.e., processing of personal data by the same controller or processor through local operations across more than one Member State – e.g., local branch offices); or

b the processing of personal data that takes place in the context of the activities of a single establishment of a controller or processor in the EU but that substantially affects or is likely to substantially affect data subjects in more than one Member State.

In determining whether the processing falls within this scope, the WP29 has published guidance stating that DSAs will interpret ‘substantially affects’ on a case-by case basis taking into account:

a the context of the processing;

b the type of data;

c whether the processing causes, or is likely to cause, damage, loss or distress to data subjects; or

d involves the processing of a wide range of personal data.

Assuming a controller is engaged in cross-border processing, it will need to carry out the main establishment test. If a controller has establishments in more than one Member State, its main establishment will be the place of its ‘central administration’ (which is not defined in the GDPR) unless this differs from the establishment in which the decisions on the purposes and means of the processing are made and implemented, in which case the main establishment will be the latter.79

For processors, the main establishment will also be the place of its central administration. However, to the extent a processor does not have a place of central administration in the EU, the main establishment will be where its main processing activities are undertaken. The WP29 in its guidance on lead supervisory authorities, make it clear that the GDPR does not

79 Article 4(16) of the GDPR.
permit ‘forum shopping’ and that where a company does not have an establishment in the EU, the one-stop-shop mechanism does not apply and it must deal with DSAs in every EU Member State in which it is active.\footnote{Article 29 Working Party, Guidelines for identifying a controller or processor’s lead supervisory authority, WP244, adopted on 13 December 2016 and revised on 5 April 2017, page 8.}

Importantly under Article 60 of the GDPR, other concerned DSAs can also be involved in the decision-making for a cross-border case. According to the GDPR, a concerned DSA will participate where:

\begin{itemize}
  \item the establishment of the controller or processor subject to the investigation is in the concerned DSA’s Member State;
  \item data subjects in the concerned DSA’s Member State are substantially or are likely to be substantially affected by the processing of the subject of the investigation; or
  \item a complaint has been lodged with that DSA.\footnote{Article 4(22) of the GDPR.}
\end{itemize}

In the case of a dispute between DSAs, the EDPB shall adopt a final binding decision.\footnote{Article 65(1) of the GDPR.} The GDPR also promotes cooperation among Member State DSAs by requiring the lead DSA to submit a draft decision on a case to the concerned DSA, where they will have to reach a consensus prior to finalising any decision.\footnote{Article 60 of the GDPR.}

**EDPB**

The EDPB is an independent EU-wide body, which contributes towards ensuring the consistent application of the GDPR across all EU Member States, and promotes cooperation between EU DSAs. The EDPB is comprised of representatives from all EU DSAs, the European Data Protection Supervisor, the EU’s independent data protection authority, and a European Commission representative, who has a right to attend EDPB meetings without voting rights.

**Enforcement rights**

The GDPR provides data subjects with a multitude of enforcement rights in relation to the processing of their personal data:

\begin{itemize}
  \item Right to lodge a complaint with the DSA: Article 77 of the GDPR provides data subjects with the right to lodge a complaint with a DSA, in the Member State of the data subject’s habitual residence, place of work or place of the alleged infringement of the GDPR, where the data subject considers that the processing of his or her personal data infringes the data protection requirements of the GDPR.
  \item Right to an effective judicial remedy against a controller or processor: Article 79 of the GDPR provides data subjects with the right to bring a claim against a controller or a processor before the courts of the Member State where the controller or processor is established in, or where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.
\end{itemize}
Right to compensation and liability: Article 82 of the GDPR provides data subjects with the right to receive compensation from the controller or processor where the data subject has suffered material or non-material damage as a result of an infringement of the GDPR.

Administrative fines

Notably, Article 83 of the GDPR grants DSAs the power to impose substantial fines on controllers or processors for the infringement of the GDPR. The GDPR provides a two-tier structure for fines, where the following will result in fines of up to €10 million or 2 per cent of annual turnover, whichever is greater:

a) failure to ensure appropriate technical and organisational measures are adopted when determining the means of processing the personal data in addition to the actual processing itself;

b) failing to comply with the Article 28(3) of the GDPR, where any processing of personal data must be governed by a written data processing agreement;

c) maintaining records as a controller of all processing activities under its responsibility;

d) conducting data protection impact assessments; and

e) notifying personal data breaches to the data subject and data supervisory authorities, respectively.85

The GDPR states that certain infringements of the GDPR merit a higher penalty and will be subject to higher fines of up to €20 million or 4 per cent of annual turnover, whichever is the greater.86 These include:

a) infringements of the basic principles of processing personal data, including conditions for obtaining consent;

b) failing to comply with data subjects’ rights requests; and

c) failing to ensure there are appropriate safeguards for the transfer of personal data outside the EEA.

These extensive penalties represent a significant change in the field of data protection that should ensure that businesses and governments take data protection compliance seriously.

DSAs’ investigative powers

DSAs also have investigative powers under Article 58(1), including the power to:

a) carry out investigations in the form of data protection audits;

b) notify the controller or processor of an alleged infringement of the GDPR; and

c) obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.

DSAs are not limited to enforcement and investigative powers, but also have corrective87 and authorisation and advisory88 powers.

85 Article 83(4) of the GDPR.
86 Article 83(5) of the GDPR.
87 Article 58(2) of the GDPR.
88 Article 58(3) of the GDPR.
**DSAs’ corrective powers**

Article 58(2) of the GDPR grants DSAs the power to require the controller or processor to make certain corrections in relation to the processing of personal data, including to:

- issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of the GDPR;
- issue reprimands to a controller or processor where processing operations have infringed provisions of the GDPR;
- order the controller or processor to comply with the data subject’s requests to exercise their data subject’s rights in accordance with the GDPR;
- order the controller or processor to bring processing operations into compliance with the provisions of the GDPR, where appropriate, in a specified manner and within a specified period;
- order the controller to communicate a personal data breach to the data subject;
- impose a temporary or definitive limitation on processing, including a ban;
- order the rectification or erasure of personal data or restriction of processing of personal data and the notification of such actions to recipients to whom the personal data has been disclosed; and
- order the suspension of data flows to a recipient in a third country.

**DSAs’ authorisation and advisory powers**

DSAs also have a range of advisory and authorisation powers under Article 58(3) of the GDPR, including the power to:

- issue opinions to the relevant Member State national parliament, Member State government or other institutions and bodies, as well as to the general public on the protection of personal data;
- authorise processing pursuant to Article 36(5) of the GDPR, if the law of the Member State requires prior authorisation;
- issue an opinion and approve draft codes of conduct pursuant to Article 40(5) of the GDPR;
- issue certifications and approve criteria of certification in accordance with Article 42(5) of the GDPR; and
- approve binding corporate rules pursuant to Article 47 of the GDPR.

**Health data under the GDPR**

Data concerning health falls within the scope of the special categories of personal data under Article 9 of the GDPR. The GDPR defines ‘data concerning health’ as ‘personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status’.89

The GDPR also states health data should include the following:

- all data pertaining to the health status of a data subject that reveals information relating to the past, current, or future physical or mental health status of the data subject;
- information collected in the course of registration for or the provision of healthcare services;

---

89 Article 4(15) of the GDPR.
c. a number, symbol, or particular assigned to an individual that uniquely identifies that individual for health purposes;

d. information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and

e. any information on disease, disability, disease risk, medical history, clinical treatment, or the physiological or biomedical state of the individual, independent of its source, for example, from a physician or a medical device.\(^90\)

Relevant in the context of health data is Article 9(2)(j) of the GDPR, which includes the legal ground regarding where the processing is necessary for scientific research purposes. To rely on this legal ground the processing must comply with Article 89(1) of the GDPR, which requires that the processing be subject to appropriate safeguards to ensure technical and organisational measures are in place and in particular, to comply with the principle of data minimisation.

### III DIRECT MARKETING

The EU Electronic Communications (Data Protection and Privacy) Directive 2002/58/EC (the ePrivacy Directive) places requirements on Member States in relation to the use of personal data for direct marketing. Direct marketing for these purposes includes unsolicited faxes, or making unsolicited telephone calls through the use of automated calling machines, or direct marketing by email. In such instances, the direct marketer needs to have the prior consent of the recipient (i.e., consent on an opt-in basis). However, in the case of emails, there are limited exceptions for email marketing to existing customers where, if certain conditions\(^91\) are satisfied, unsolicited emails can still be sent without prior consent. In other instances of unsolicited communications, it is left up to each Member State to decide whether such communications will require the recipient’s prior consent or can be sent without prior consent unless recipients have indicated that they do not wish to receive such communications (i.e., consent on an opt-out basis).\(^92\)

The ePrivacy Directive imposes requirements on providers of publicly available electronic communication services to put in place appropriate security measures and to notify subscribers of certain security breaches in relation to personal data.\(^93\) The ePrivacy Directive was also amended in 2009\(^94\) to require that website operators obtain the informed consent of users to collect personal data of users through website ‘cookies’ or similar technologies used for storing information. There are two exemptions to the requirement to obtain consent before using cookies: when the cookie is used for the sole purpose of carrying out the transmission

---

90 Recital 35 of the GDPR.

91 Unsolicited emails may be sent without prior consent to existing customers if the contact details of the customer have been obtained in the context of a sale of a product or a service and the unsolicited email is for similar products or services; and if the customer has been given an opportunity to object, free of charge in an easy manner, to such use of his or her electronic contact details when they are collected and on the occasion of each message in the event the customer has not initially refused such use – Article 13(2) of the ePrivacy Directive.

92 Article 13(3) of the ePrivacy Directive.

93 Recital 20 and Article 4 of the ePrivacy Directive.

94 Directive 2009/56/EC.
of a communication over an electronic communications network; and when the cookie is strictly necessary for the provider of an information society service explicitly requested by the subscriber or user to provide the service.\footnote{Article 5(3) of the ePrivacy Directive.}

The WP29 has published an opinion on the cookie consent exemption\footnote{WP 194 – Opinion 04/2012 on Cookie Consent Exemption.} that provides an explanation on which cookies require the consent of website users (e.g., social plug-in tracking cookies, third-party advertising cookies used for behavioural advertising, analytics) and those that fall within the scope of the exemption (e.g., authentication cookies, multimedia player session cookies and cookies used to detect repeated failed login attempts). Guidance on how to obtain consent has been published at a national level by various data protection authorities.\footnote{For example: UK Information Commissioner’s Office, ‘Guidance on the rules on use of cookies and similar technologies’; and the French Commission Nationale de l’Informatique et des Libertés.}

In July 2016, the Article 29 Working Party issued an opinion on a revision of the rules contained in the ePrivacy Directive.\footnote{Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC).}

On 10 January 2017, the European Commission issued a draft of the proposed Regulation on Privacy and Electronic Communications (the ePrivacy Regulation) to replace the existing ePrivacy Directive.\footnote{Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications).} The ePrivacy Regulation will complement the Regulation and provide additional sector-specific rules, including in relation to marketing and the use of website cookies.

The key changes in the proposed ePrivacy Regulation will:

\begin{enumerate}
\item require a clear affirmative action to consent to cookies;
\item attempt to encourage the shifting of the burden of obtaining consent for cookie use to website browsers; and
\item ensuring that consent for direct marketing will be harder to obtain and must meet the standard set out in the Regulation; however, existing exceptions, such as the exemption where there is an existing relationship and similar products and services are being marketed, are likely to be retained.
\end{enumerate}

The European Commission’s original timetable for the ePrivacy Regulation was for it to apply from 25 May 2018 and coincide with the coming into force of the GDPR. However, owing to ongoing political negotiations between the European Council (which represents EU Member States) and the European Parliament, the ePrivacy Regulation is not expected to come into force until 2019 at the earliest.

In April 2017, the Article 29 Working Party issued an opinion on the proposed ePrivacy Regulation, which welcomed some elements of the proposal but also identified areas of ‘grave concern’, including with regard to cookie tracking walls.\footnote{Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC).} The EDPB published a statement on 25 May 2018 noting the ‘widespread’ use of ‘over-the-top’ services, which bypass traditional forms of distribution such as cable or satellite pay-TV services, for internet-based
content-distribution services and formed the view that the ePrivacy Regulation ‘should provide protection for all types of electronic communications, including those carried out by “Over-the-Top Services”’.

IV CLOUD COMPUTING

In its guidance on cloud computing adopted on 1 July 2012, the EU’s WP29 states that the majority of data protection risks can be divided into two main categories: lack of control over the data; and insufficient information regarding the processing operation itself. The lawfulness of the processing of personal data in the cloud depends on adherence to the principles of the now repealed EU Data Protection Directive that are considered in the WP29 opinion, and some of which are summarised below. It would be reasonable to expect that the EDPB will issue new guidance on cloud computing and data protection to reflect new requirements under the GDPR. For the purposes of this section, references to the Data Protection Directive should be read as references to the GDPR.

i Instructions of the data controller

To comply with the requirements of the EU Data Protection Directive, the WP29 provides that the extent of the instructions should be detailed in the relevant cloud computing agreement (the cloud agreement) along with service levels and financial penalties on the provider for non-compliance.

ii Purpose specification and limitation requirement

Under Article 6(b) of the Data Protection Directive, personal data must be collected for specified, explicit and legitimate purposes, and not further processed in a way that is incompatible with those purposes. To address this requirement, the agreement between the cloud provider and the client should include technical and organisational measures to mitigate this risk and provide assurances for the logging and auditing of relevant processing operations on personal data that are performed by employees of the cloud provider or subcontractors.

iii Security

Under the Data Protection Directive, a data controller must have in place adequate organisational and technical security measures to protect personal data and should be able to demonstrate accountability. The WP29 opinion comments on this point, reiterating that it is of great importance that concrete technical and organisational measures are specified in the cloud agreement, such as availability, confidentiality, integrity, isolation and portability. As a consequence, the agreement with the cloud provider should contain a provision to ensure that the cloud provider and its subcontractors comply with the security measures imposed by the client. It should also contain a section regarding the assessment of the security measures.

101 Statement of the EDPB on the revision of the ePrivacy Regulation and its impact on the protection of individuals with regard to the privacy and confidentiality of their communications.
103 Article 6(b) of the Data Protection Directive.
104 Article 17(2) of the Data Protection Directive.
of the cloud provider. The agreement should also contain an obligation for the cloud provider to inform the client of any security event. The client should also be able to assess the security measures put in place by the cloud provider.

iv  **Subcontractors**

The WP29 opinion indicates that sub-processors may only be commissioned on the basis of a consent that can be generally given by the controller in line with a clear duty for the processor to inform the controller of any intended changes in this regard, with the controller retaining at all times the possibility to object to the changes or to terminate the agreement. There should also be a clear obligation on the cloud provider to name all the subcontractors commissioned, as well as the location of all data centres where the client’s data can be hosted. It must also be guaranteed that the cloud provider and all the subcontractors shall act only on instructions from the client. The agreement should also set out the obligation on the part of the processor to deal with international transfers, for example, by signing contracts with sub-processors, based on the EU model contract clauses.

v  **Erasure of data**\(^{105}\)

The WP29 opinion states that specifications on the conditions for returning the personal data or destroying the data once the service is concluded should be contained in the agreement. It also states that data processors must ensure that personal data are erased securely at the request of the client.

vi  **Data subjects’ rights**\(^{106}\)

According to the WP29 opinion, the agreement should stipulate that the cloud provider is obliged to support the client in facilitating exercise of data subjects’ rights to access, correct or delete their data, and to ensure that the same holds true for the relation to any subcontractor.

vii  **International transfers**\(^{107}\)

As discussed above, under Articles 25 and 26 of the Data Protection Directive, personal data can only be transferred to countries located outside the EEA if the country provides an adequate level of protection.

viii  **Confidentiality**

The WP29 opinion recommends that an agreement with the cloud provider should contain confidentiality wording that is binding both upon the cloud provider and any of its employees who may be able to access the data.

ix  **Request for disclosure of personal data by a law enforcement authority**

Under the WP29 opinion, the client should be notified of any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as under a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation.

---

105  Article 6(e) of Data Protection Directive.
x Changes concerning the cloud services

The WP29 recommends that the agreement with the cloud provider should contain a provision stating that the cloud provider must inform the client about relevant changes concerning the cloud service concerned, such as the implementation of additional functions.

Now that the GDPR is in effect, clients and cloud service providers will need to be mindful that references to the Data Protection Directive in the WP29 opinion will be defunct and that the equivalent principles and requirements in the GDPR should be complied with instead. For example, under Article 28(3) of the GDPR, processing by the processor (i.e., the cloud service provider) must be governed by a contract with the controller that stipulates a number of obligations set out by the GDPR.

V WHISTLE-BLOWING HOTLINES

The WP29 published an Opinion in 2006 on the application of the EU data protection rules to whistle-blowing hotlines providing various recommendations under the now repealed Data Protection Directive, which are summarised below. It would be reasonable to expect that the EDPB will issue new guidance on whistle-blowing hotlines to reflect new requirements under the GDPR. For the purposes of this section, references to the Data Protection Directive should be read as references to the GDPR.

i Legitimacy of whistle-blowing schemes

Under the GDPR, personal data must be processed fairly and lawfully. For a whistle-blowing scheme, this means that the processing of personal data must be on the basis of at least one of certain grounds, the most relevant of which include where:

a the processing is necessary for compliance with a legal obligation to which the data controller is subject, which could arguably include a company’s obligation to comply with the provisions of the US Sarbanes-Oxley Act (SOX). However, the WP29 concluded that an obligation imposed by a foreign statute, such as SOX, does not qualify as a legal obligation that would legitimise the data processing in the EU; or

b the processing is necessary for the purposes of the legitimate interests pursued by the data controller, or by the third party or parties to whom the data are disclosed, except where those interests are overridden by the interests or the fundamental rights and freedoms of the data subject. The WP29 acknowledged that whistle-blowing schemes adopted to ensure the stability of financial markets, and in particular the prevention of fraud and misconduct in respect of accounting, internal accounting controls, auditing matters and reporting as well as the fight against bribery, banking and financial crime, or insider trading, might be seen as serving a legitimate interest of a company that would justify the processing of personal data by means of such schemes.

ii Limiting the number of persons eligible to use the hotline

Applying the proportionality principle, the WP29 recommends that the company responsible for the whistle-blowing reporting programme should carefully assess whether it might

---

WP 117 – Opinion 1/2006 on the application of EU data protection rules to internal whistle-blowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime.
be appropriate to limit the number of persons eligible for reporting alleged misconduct and the number of persons who might be incriminated. However, the recommendations acknowledged that in both cases the categories of personnel involved may still sometimes include all employees in the fields of accounting, auditing and financial services.

### iii Promotion of identified reports

The WP29 pointed out that, although in many cases anonymous reporting is a desirable option, where possible, whistle-blowing schemes should be designed in such a way that they do not encourage anonymous reporting. Rather, the helpline should obtain the contact details of reports and maintain the confidentiality of that information within the company, for those who have a specific need to know the relevant information. The WP29 opinion also suggested that only reports that included information identifying the whistle-blower would be considered as satisfying the essential requirement that personal data should only be processed ‘fairly’.

### iv Proportionality and accuracy of data collected

Companies should clearly define the type of information to be disclosed through the system by limiting the information to accounting, internal accounting control or auditing, or banking and financial crime and anti-bribery. The personal data should be limited to data strictly and objectively necessary to verify the allegations made. In addition, complaint reports should be kept separate from other personal data.

### v Compliance with data-retention periods

According to the WP29, personal data processed by a whistle-blowing scheme should be deleted promptly and usually within two months of completion of the investigation of the facts alleged in the report. These periods would be different when legal proceedings or disciplinary measures are initiated. In such cases, personal data should be kept until the conclusion of these proceedings and the period allowed for any appeal. Personal data found to be unsubstantiated should be deleted without delay.

### vi Provision of clear and complete information about the whistle-blowing programme

Companies as data controllers must provide information to employees about the existence, purpose and operation of the whistle-blowing programme, the recipients of the reports and the right of access, rectification and erasure for reported persons. Users should also be informed that the identity of the whistle-blower shall be kept confidential, that abuse of the system may result in action against the perpetrator of that abuse and that they will not face any sanctions if they use the system in good faith.

### vii Rights of the incriminated person

The WP29 noted that it was essential to balance the rights of the incriminated person and of the whistle-blower and the company’s legitimate investigative needs. In accordance with the Data Protection Directive, an accused person should be informed by the person in charge of the ethics reporting programme as soon as practicably possible after the ethics report implicating them is received. The implicated employee should be informed about:

- the entity responsible for the ethics reporting programme;
the acts of which he or she is accused;
c. the departments or services that might receive the report within the company or in other entities or companies of the corporate group; and
d. how to exercise his or her rights of access and rectification.

Where there is a substantial risk that such notification would jeopardise the ability of the company to effectively investigate the allegation or gather evidence, then notification to the incriminated person may be delayed as long as the risk exists.

The whistle-blowing scheme also needs to ensure compliance with the individual’s right, under the Data Protection Directive, of access to personal data on them and their right to rectify incorrect, incomplete or outdated data. However, the exercise of these rights may be restricted to protect the rights of others involved in the scheme and under no circumstances can the accused person obtain information about the identity of the whistle-blower, except where the whistle-blower maliciously makes a false statement.

viii Security
The company responsible for the whistle-blowing scheme must take all reasonable technical and organisational precautions to preserve the security of the data and to protect against accidental or unlawful destruction or accidental loss and unauthorised disclosure or access. Where the whistle-blowing scheme is run by an external service provider, the EU data controller needs to have in place a data processing agreement and must take all appropriate measures to guarantee the security of the information processed throughout the whole process and commit themselves to complying with the data protection principles.

ix Management of whistle-blowing hotlines
A whistle-blowing scheme needs to carefully consider how reports are to be collected and handled with a specific organisation set up to handle the whistle-blower’s reports and lead the investigation. This organisation must be composed of specifically trained and dedicated people, limited in number and contractually bound by specific confidentiality obligations. The whistle-blowing system should be strictly separated from other departments of the company, such as human resources.

x Data transfers from the EEA
The WP29 believes that groups should deal with reports locally in one EEA state rather than automatically share all the information with other group companies. However, data may be communicated within the group if the communication is necessary for the investigation, depending on the nature or seriousness of the reported misconduct or results from how the group is set up. The communication will be considered necessary, for example, if the report incriminates another legal entity within the group involving a high-level member of management of the company concerned. In this case, data must only be communicated under confidential and secure conditions to the competent organisation of the recipient entity, which provides equivalent guarantees as regards management of the whistle-blowing reports as the EU organisation.
VI E-DISCOVERY

The WP29 has published a working document providing guidance to data controllers in dealing with requests to transfer personal data to other jurisdictions outside the EEA for use in civil litigation and to help them to reconcile the demands of a litigation process in a foreign jurisdiction with EU data protection obligations.

The main suggestions and guidelines include the following:

a. Possible legal bases for processing personal data as part of a pretrial e-discovery procedure include consent of the data subject and compliance with a legal obligation. However, the WP29 states that an obligation imposed by a foreign statute or regulation may not qualify as a legal obligation by virtue of which data processing in the EU would be made legitimate. A third possible basis is a legitimate interest pursued by the data controller or by the third party to whom the data are disclosed where the legitimate interests are not overridden by the fundamental rights and freedoms of the data subjects. This involves a balance-of-interest test taking into account issues of proportionality, the relevance of the personal data to litigation and the consequences for the data subject.

b. Restricting the disclosure of data if possible to anonymised or redacted data as an initial step and after culling the irrelevant data, disclosing a limited set of personal data as a second step.

c. Notifying individuals in advance of the possible use of their data for litigation purposes and, where the personal data is actually processed for litigation, notifying the data subject of the identity of the recipients, the purposes of the processing, the categories of data concerned and the existence of their rights.

d. Where the non-EEA country to which the data will be sent does not provide an adequate level of data protection, and where the transfer is likely to be a single transfer of all relevant information, then there would be a possible ground that the transfer is necessary for the establishment, exercise or defence of a legal claim. Where a significant amount of data is to be transferred, the WP29 previously suggested the use of binding corporate rules or the Safe Harbor regime. However, Safe Harbor was found to be invalid by the CJEU in 2015. The Safe Harbor regime was, however, effectively replaced on 12 July 2016 by the Privacy Shield. In the absence of any updates from the WP29 to its e-discovery working document, it can be assumed that the use of Privacy Shield is also an appropriate means of transferring significant amounts of data. It also recognises that compliance with a request made under the Hague Convention would provide a formal basis for the transfer of the data.

It would be reasonable to expect that the EDPB will issue new guidance on e-discovery, in light of the entry into force of Article 48 of the GDPR.

Article 48 of the GDPR facilitates the transfer of personal data from the EU to a third country on the basis of a judgment of a court or tribunal or any decision of an administrative authority of a third country where the transfer is based on a mutual legal assistance treaty (MLAT) between the requesting third country and the EU Member State concerned. As

110 Article 48 of the GDPR.
MLATs between EU Member States and third countries are not widespread, there is a further exception for data controllers to rely on. The GDPR states that the restrictive requirements in which a judicial or administrative request from a third country to transfer personal data from the EU to that third country is only permissible on the basis of an MLAT, is ‘without prejudice to other grounds for transfer’ in the GDPR.

Accordingly, this enables data controllers in the EU facing e-discovery requests to transfer personal data to a jurisdiction outside of the EU to rely on transfer mechanisms such as EU standard contractual clauses and binding corporate rules. In the absence of a transfer mechanism, the GDPR provides certain derogations for several specific situations in which personal data can in fact be transferred outside the EEA:

- where the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- the transfer is necessary for the performance of a contract between the data subject and the controller;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject;
- the transfer is necessary for important reasons of public interest under EU law or the law of the Member State in which the controller is subject;
- the transfer is necessary for the establishment, exercise or defence of legal claims;
- the transfer is necessary to protect the vital interests of the data subject, where the data subject is physically or legally incapable of giving consent; and
- the transfer is made on the basis of compelling legitimate interests of the controller, provided the transfer is not repetitive and only concerns a limited number of data subjects.\(^{111}\)

### VII EU CYBERSECURITY STRATEGY

In March 2014, the European Parliament adopted a proposal for the NIS Directive,\(^{112}\) which was proposed by the European Commission in 2013. The NIS Directive is part of the European Union’s Cybersecurity Strategy aimed at tackling network and information security incidents and risks across the EU and was adopted on 6 June 2016 by the European Parliament at second reading.\(^{113}\)

The main elements of the NIS Directive include:

- new requirements for ‘operators of essential service’ and ‘digital service providers’;
- a new national strategy;
- designation of a national competent authority; and
- designation of computer security incident response teams (CSIRTs) and a cooperation network.

---

111 Article 49 of the GDPR.
112 Proposal for a directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, 7 February 2013.
i  **New national strategy**

The NIS Directive requires Member States to adopt a national strategy setting out concrete policy and regulatory measures to maintain a high level of network and information security.\(^{114}\) This includes having research and development plans in place or a risk assessment plan to identify risks, designating a national competent authority that will be responsible for monitoring compliance with the NIS Directive and receiving any information security incident notifications,\(^{115}\) and setting up of at least one CSIRT that is responsible for handling risks and incidents.\(^{116}\)

ii  **Cooperation network**

The competent authorities in EU Member States, the European Commission and ENISA will form a cooperation network to coordinate against risks and incidents affecting network and information systems.\(^{117}\) The cooperation network will exchange information between authorities and also provide early warnings on information security risks and incidents, and agree on a coordinated response in accordance with an EU–NIS cyber-cooperation plan.

iii  **Security requirements**

A key element of the NIS Directive is that Member States must ensure public bodies and certain market operators\(^{118}\) take appropriate technical and organisational measures to manage the security risks to networks and information systems, and to guarantee a level of security appropriate to the risks.\(^{119}\) The measures should prevent and minimise the impact of security incidents affecting the core services they provide. Public bodies and market operators must also notify the competent authority of incidents having a significant impact on the continuity of the core services they provide, and the competent authority may decide to inform the public of the incident. The significance of the disruptive incident should take into account:

- the number of users affected;
- the dependency of other key market operators on the service provided by the entity;
- the duration of the incident;
- the geographic spread of the area affected by the incident;
- the market share of the entity; and
- the importance of the entity for maintaining a sufficient level of service, taking into account the availability of alternative means for the provisions of that service.

Member States had until May 2018 to implement the NIS Directive into their national laws.

---

114  Article 7 of the NIS Directive.
115  Article 8 of the NIS Directive.
116  Article 9 of the NIS Directive.
117  Article 11 of the NIS Directive.
118  Operators of essential services are listed in Annex II of the NIS Directive and include operators in energy and transport, financial market infrastructures, banking, operators in the production and supply of water, the health sector and digital infrastructure. Digital service providers (e.g., e-commerce platforms, internet payment gateways, social networks, search engines, cloud computing services and application stores) are listed in Annex III. The requirements for digital service providers are less onerous than those imposed on operators of essential services; however, they are still required to report security incidents that have a significant impact on the service they offer in the EU.
119  Article 14 of the proposed NIS Directive.
Organisations should review the provisions of the NIS Directive and of any draft or finalised Member State implementing legislation and begin amending their cybersecurity practices and procedures to ensure compliance.

iv  New Cybersecurity Act

On 13 September 2017, the European Commission introduced proposals for an EU Cybersecurity Act (Act) that would impose an EU-wide cybersecurity certification scheme for the purposes of ensuring an adequate level of cybersecurity of information and communication technology (ICT) products and services across the EU. The Act would introduce a set of technical requirements and rules relating to the production of certifications for ICT devices, or products, ranging from smart medical devices and connected cars to video game consoles and fire alarms. The proposed Act is part of the European Union’s push towards a digital single market.

Under the Act, ENISA would be granted more oversight powers in relation to ensuring a uniform cybersecurity policy in the EU. ENISA currently serves as a body of expertise on cybersecurity. If the Act were to come into force, ENISA would become a permanent EU cybersecurity agency and would get new powers to provide effective and efficient support to EU Member States and EU institutions on cybersecurity issues and to ensure a secure cyberspace across the EU. In addition, ENISA would be responsible for carrying out product certifications, with certifications voluntary for companies unless otherwise stated in EU or Member State law. The EU wide cybersecurity certification framework for ICT products and services would allow certificates to be issued by ENISA ensuring an adequate level of cybersecurity for the ICT products and services, which would be valid and recognised across all EU Member States, and serve to address the current market and Member State fragmentation in relation to cybersecurity certifications for ICT products and services.

The Act is currently the subject of negotiations between the European Council and the European Parliament.

VIII  OUTLOOK

The past 12 months have seen a number of key developments in the European data protection world, most notable is the entry into force of the GDPR, described as the most lobbied piece of European legislation in history, receiving over 4,000 amendments in opinions from committees in the European Parliament as well as from numerous industries. The EDPB has begun to issue guidance on aspects of the GDPR. To date, the EDPB has published guidance on the certification criteria for international data transfers and on Article 48 of the GDPR. These guidance documents, together with those published by Member State DSAs should provide businesses with a clearer sense of how to comply with the GDPR in practice.

Data subjects in the EU have made use of the substantial data protection rights provided by the GDPR at a rapid pace. On the day the GDPR came into force, privacy campaigner Max Schrems and his non-profit organisation None of Your Business filed four complaints with two Member State DSAs against two global technology companies for infringing the data protection requirements of the GDPR, in particular its obligation, when relying on consent as a lawful processing ground, to obtain informed and specific consent.

Additionally, the adoption of the GDPR was intended to harmonise data protection laws across all EU Member States. However, there is growing concern over significant national divergences of data protection laws in EU Member States, in particular with the application
and interpretation of the GDPR. One area where national divergence of data protection could cause potential problems, is in the life sciences sector due to the national derogations in the GDPR that allow Member States to introduce further conditions with regard to the processing of health data.

A key development in the framework of European data protection and an area to watch is Brexit and the UK’s departure from the EU on 29 March 2019 and its attempts to agree on a potential adequacy agreement with the European Commission in relation to the lawful transfer of personal data from the EEA to the UK. This is because on 29 March 2019, the UK will become a third country and will face restrictions on any transfer and processing of personal data of EU data subjects from the EEA to the UK.
I OVERVIEW

The Asia-Pacific Economic Cooperation (APEC) is an organisation of economic entities in the Asia-Pacific region formed to enhance economic growth and prosperity in the region. It was established in 1989 by 12 Asia-Pacific economies as an informal ministerial-level dialogue group. Because APEC is primarily concerned with trade and economic issues, the criterion for membership is being an economic entity rather than a nation. For this reason, its members are usually described as ‘APEC member economies’ or ‘APEC economies’. Since 1993, the heads of the member economies have met annually at an APEC Economic Leaders Meeting, which has since grown to include 21 member economies as of July 2018: Australia, Brunei, Canada, Chile, China, Hong Kong, Indonesia, Japan, Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, the Philippines, Russia, Singapore, Taiwan, Thailand, the United States and Vietnam. Collectively, the 21 member economies account for more than half of world real GDP in purchasing power parity and over 44 per cent of total world trade.

The main aim of APEC is to fulfil the goals established in 1994 at the Economic Leaders Meeting in Bogor, Indonesia of free and open trade and investment in the Asia-Pacific area for both industrialised and developing economies. APEC established a framework of key areas of cooperation to facilitate achievement of these ‘Bogor Goals’. These areas, also known as the three pillars of APEC, are the liberalisation of trade and investment, business facilitation and economic and technical cooperation. In recognition of the exponential growth and transformative nature of electronic commerce, and its contribution to economic growth in the region, APEC established an Electronic Commerce Steering Group (ECSG) in 1999, which began to work towards the development of consistent legal, regulatory and policy...
environments in the Asia-Pacific area. It further established the Data Privacy Subgroup under the ECSG in 2003 to address privacy and other issues identified in the 1998 APEC Blueprint for Action on Economic Commerce.

Because of varied domestic privacy laws among the member economies (including economies at different stages of legislative recognition of privacy), APEC concluded that a regional agreement that creates a minimum privacy standard would be the optimal mechanism for facilitating the free flow of data among the member economies (and thus promoting electronic commerce). The result was the principles-based APEC Privacy Framework, which was endorsed by the APEC economies in 2005. Although consistent with the original Organisation for Economic Co-operation and Development (OECD) Guidelines, the APEC Privacy Framework also provided assistance to member economies in developing data privacy approaches that would optimise the balance between privacy protection and cross-border data flows.

Unlike other privacy frameworks, APEC does not impose treaty obligation requirements on its member economies. Instead, the cooperative process among APEC economies relies on non-binding commitments, open dialogue and consensus. Member economies undertake commitments on a voluntary basis. Consistent with this approach, the APEC Privacy Framework is advisory only and thus has few legal requirements or constraints.

In 2011, APEC implemented the Cross-Border Privacy Rules (CBPR) system, under which companies trading within the member economies develop their own internal business rules consistent with the APEC privacy principles to secure cross-border data privacy. In 2015, APEC developed the Privacy Recognition for Processors (PRP) system, a corollary to the CBPR system for data processors. APEC is also working with the EU to study the potential interoperability of the APEC and the EU’s new General Data Protection Regulation (GDPR), building upon the issuance in 2014 of a joint referential document mapping requirements of APEC and the EU’s former data protection regime.

The APEC Privacy Framework, the CBPR and PRP systems, the cooperative privacy enforcement system and APEC–EU collaborative efforts are all described in more detail below.

II APEC PRIVACY FRAMEWORK

i Introduction

The APEC Privacy Framework, endorsed by APEC in 2005, was developed to promote a consistent approach to information privacy protection in the Asia-Pacific region as a means of ensuring the free flow of information in support of economic development. It was an outgrowth of the 1998 APEC Blueprint for Action on Electronic Commerce, which recognised that the APEC member economies needed to develop and implement legal and
regulatory structures to build public confidence in the safety and security of electronic data flows (including consumers’ personal data) to realise the potential of electronic commerce. This recognition was the impetus behind the development of the Privacy Framework. Thus, the APEC objective of protecting informational privacy arises in the context of promoting trade and investment, rather than primarily to protect basic human rights as in the European Union.

The APEC Privacy Framework represents a consensus among economies with different legal systems, cultures and values, and that at the time of endorsement were at different stages of adoption of domestic privacy laws and regulations. Thus, the Framework provided a basis for the APEC member economies to acknowledge and implement basic principles of privacy protection, while still permitting variation among them. It further provides a common basis on which to address privacy issues in the context of economic growth and development, both among the member economies and between them and other trading entities. The Privacy Framework was updated in 2015 to account for the development of new technologies and developments in the marketplace and to ensure that the free flow of information and data across borders is balanced with effective data protections. While updates were made to the preamble and commentary sections, the basic principles of the Framework remained unchanged. Further updates to the Privacy Framework are in the planning stages.

ii  The Privacy Framework

The Privacy Framework has four parts:

a  Part I is a preamble that sets out the objectives of the principles-based Privacy Framework and discusses the basis on which consensus was reached;
b  Part II describes the scope of the Privacy Framework and the extent of its coverage;
c  Part III sets out the information privacy principles, including an explanatory commentary on them; and
d  Part IV discusses the implementation of the Privacy Framework, including providing guidance to member economies on options for domestic implementation.

Objectives and scope of the Privacy Framework (Parts I and II)

The market-oriented approach to data protection is reflected in the objectives of the Privacy Framework, which include – in addition to the protection of information – the prevention of unnecessary barriers to information flows, the promotion of uniform approaches by multinational businesses to the collection and use of data, and the facilitation of domestic and international efforts to promote and enforce information privacy protections. The Privacy Framework was designed for broad-based acceptance across member economies by encouraging compatibility while still respecting the different cultural, social and economic requirements within the economies. As such, it sets an advisory minimum standard and permits member economies to adopt stronger, country-specific data protection laws.

The Privacy Framework cautions that the principles should be interpreted as a whole, rather than individually, because they are interconnected, particularly in how they balance privacy rights and the market-oriented public interest. These principles are not intended to

---

impede governmental activities within the member economies that are authorised by law, and thus the principles allow exceptions that will be consistent with particular domestic circumstances.8 The Framework specifically recognises that there ‘should be flexibility in implementing these Principles’.9

The nine principles of the Privacy Framework (Part III)

Given that seven of the original APEC member economies were members of the OECD, it is not surprising that the original APEC Privacy Framework was based on the original OECD Guidelines. Similarly, the 2015 update was based on a 2013 update to the OECD’s Guidelines.10 The APEC privacy principles address personal information about living individuals and exclude both publicly available information and information connected with domestic affairs. The principles apply to persons or organisations in both public and private sectors who control the collection, holding, processing or use of personal information. Organisations that act as agents for others are excluded from compliance.

While based on the OECD Guidelines, the APEC principles are not identical to them. Missing are the OECD Guidelines of ‘purpose specification’ and ‘openness’, although aspects of these can be found within the nine principles – for example, purpose limitations are incorporated in Principle IV regarding use of information. The APEC principles also permit a broader scope of exceptions and are slightly stronger than the OECD Guidelines on notice. In general, the APEC principles reflect the objective of promoting economic development and the respect for differing legal and social values among the member economies.

Principle I – preventing harm

This principle provides that privacy protections be designed to prevent harm to individuals from wrongful collection or misuse of their personal information and that remedies for infringement be proportionate to the likelihood and severity of harm.

Principle II – notice

The notice principle addresses the information that a data controller must include in a notice to individuals when collecting their personal information. It also requires that all reasonable steps be taken to provide the notice either before or at the time of collection and if not, then as soon after collection as is reasonably practicable. The principle further provides for an exception for notice of collection and use of publicly available information.

Principle III – collection limitation

This principle provides for the lawful and fair collection of personal information limited to that which is relevant to the purpose of collection and, where appropriate, with notice to, or consent of, the data subject.

9 See APEC Privacy Framework (2015), Paragraph 17.
Principle IV – uses of personal information
This principle limits the use of personal information to those uses that fulfil the purpose of collection and other compatible or related purposes. It includes exceptions for information collected with the consent of the data subject and collection necessary to complete a request of the data subject or as required by law.

Principle V – choice
The choice principle directs that, where appropriate, individuals be provided with mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information, with an exception for publicly available information. This principle also contemplates that, in some instances, consent can be implied or is not necessary.

Principle VI – integrity of personal information
This principle states that personal information should be accurate, complete and kept up to date to the extent necessary for the purpose of use.

Principle VII – security safeguards
This principle requires that security safeguards be applied to personal data that are appropriate and proportional to the likelihood and severity of threatened harm, the sensitivity of the data and the context in which it is held, and that the safeguards be periodically reassessed.

Principle VIII – access and correction
The access and correction principle directs that individuals have the right of access to their personal information within a reasonable time and in a reasonable manner, and may challenge its accuracy and request appropriate correction. This principle includes exceptions when the burden of access or correction outweighs the risks to individual privacy, the information is subject to legal or security holds, or where privacy rights of other data subjects may be affected.

Principle IX – accountability
This principle requires that a data controller be accountable for complying with measures that give effect to the nine principles and that, when transferring personal information, it should take reasonable steps to ensure that the recipients also protect the information in a manner that is consistent with the principles. This has often been described as the most important innovation in the APEC Privacy Framework and it has been influential in encouraging other privacy regulators to consider similar accountability processes tailored to the risks associated with that specific data.

Unlike other international frameworks, the APEC Privacy Framework neither restricts the transfer of data to countries without APEC-compliant data protection laws nor requires such a transfer to countries with APEC-compliant laws. Instead, APEC adopted the accountability principle in lieu of data import and export limitations as being more consistent with modern business practices and the stated objectives of the Privacy Framework.

Implementation (Part IV)
Because APEC is a cooperative organisation, the member economies are not required to convert the Privacy Framework into domestic legislation. Rather, the Privacy Framework encourages
the member economies to implement it without requiring or proposing any particular means of doing so. It suggests that there are ‘several options for giving effect to the Framework […] including legislative, administrative, industry self-regulatory or a combination of these policy instruments’. The Framework advocates ‘having a range of remedies commensurate with the extent of the actual or potential harm to individuals resulting from […] violations’ and supports a choice of remedies appropriate to each member economy. The Privacy Framework does not contemplate a central enforcement entity.

Thus, the APEC Privacy Framework contemplates variances in implementation across member economies. It encourages member economies to share information, surveys and research and to expand their use of cooperative arrangements (such as the Cross-Border Privacy Enforcement Arrangement (CPEA (see Section III.iii)) to facilitate cross-border cooperation in investigation and enforcement.

### III APEC CROSS-BORDER DATA TRANSFER

#### i Data Privacy Pathfinder initiative

When originally enacted in 2005, the APEC Privacy Framework did not explicitly address the issue of cross-border data transfer, but rather called for cooperative development of cross-border privacy rules. In 2007, the APEC ministers endorsed the APEC Data Privacy Pathfinder initiative with the goal of achieving accountable cross-border flows of personal information within the Asia-Pacific region. The Data Privacy Pathfinder initiative contains general commitments leading to the development of an APEC CBPR system that would support accountable cross-border data flows consistent with the APEC Privacy Principles.

The main objectives of the Pathfinder initiative are to promote a conceptual framework of principles for the execution of cross-border privacy rules across APEC economies, to develop consultative processes among the stakeholders in APEC member economies for the development of implementing procedures and documents supporting cross-border privacy rules and to implement an accountable cross-border privacy system. Both the CBPR system and the CPEA – cross-border privacy systems that facilitate data protection and privacy enforcement – are outcomes of the Pathfinder initiative.

---

13 See APEC Privacy Framework (2015), Paragraphs 57–64.
17 See Sections III.ii and III.iii
**The CBPR system**

The APEC CBPR system, endorsed in 2011, is a voluntary accountability-based system governing electronic flows of private data among APEC economies. As of July 2018, six APEC economies participate in the CBPR system – Canada, Japan, Mexico, South Korea, Singapore (a recent addition) and the United States – with more expected to join.\(^{18}\)

In general, the CBPR system requires businesses to develop their own internal privacy-based rules governing the transfer of personal data across borders under standards that meet or exceed the APEC Privacy Framework. The system is designed to build consumer, business and regulator trust in the cross-border flow of electronic personal data in the Asia-Pacific region. One of the goals of the CBPR system is to ‘lift the overall standard of privacy protection throughout the [Asia-Pacific] region’ through voluntary, enforceable standards set out within it.\(^{19}\)

Organisations that choose to participate in the CBPR system must submit their privacy practices and policies for evaluation by an APEC-recognised accountability agent to assess compliance with the programme. Upon certification, the practices and policies will become binding on that organisation and enforceable through the relevant privacy enforcement authority.\(^{20}\)

The CBPR system is governed by the Data Privacy Subgroup, which administers the programme through the Joint Oversight Panel, which is composed of nominated representatives of participating economies and any working groups the Panel establishes. The Joint Oversight Panel operates according to the Charter of the APEC Cross-Border Privacy Rules and Privacy Recognition for Processors Systems Joint Oversight Panel and the Protocols of the APEC Cross-Border Privacy Rules System Joint Oversight Panel.\(^{21}\)

Accountability agents and privacy enforcement authorities are responsible for enforcing the CBPR programme requirements, either under contract (private accountability agents) or under applicable domestic laws and regulations (accountability agents and privacy enforcement authorities).

The CBPR system has its own website, which includes general information about the system, charters and protocols, lists of current participants and certified entities, submissions and findings reports and template forms.\(^{22}\)

**Participation in the CBPR system**

Only APEC member economies may participate in the CBPR system and must meet three requirements:

\(^{a}\) participation in the APEC CPEA with at least one privacy enforcement authority;

---

18 https://www.huntonprivacyblog.com/2018/03/08/singapore-joins-the-apec-cbpr-and-prp-systems/#more-14134 (Australia, the Philippines and Chinese Taipei are actively working to join CBPR and PRP systems).


20 A privacy enforcement authority is ‘any public body that is responsible for enforcing Privacy Law, and that has powers to conduct investigations or pursue enforcement proceedings’. ‘Privacy Law’ is further defined as ‘laws and regulations of an APEC Economy, the enforcement of which have the effect of protecting personal information consistent with the APEC Privacy Framework’. APEC Cross-Border Privacy Rules System, Policies, Rules and Guidelines, at 10.

21 See cbprs.blob.core.windows.net/files/JOP%20Charter.pdf; and cbprs.blob.core.windows.net/files/JOP%20Protocols.pdf.

22 See www.cbprs.org/default.aspx.
b. submission of a letter of intent to participate addressed to the chairs of the APEC ECSG, the Data Privacy Subgroup and the CBPR system Joint Oversight Panel providing:
• confirmation of CPEA participation;
• identification of the APEC CBPR system-recognised accountability agent that the economy intends to use;
• details regarding relevant domestic laws and regulations, enforcement entities and enforcement procedures; and

c. submission of the APEC CBPR system programme requirements enforcement map.

The Joint Oversight Panel of the CBPR issues a findings report that addresses whether the economy has met the requirements for becoming an APEC CBPR system participant. An applicant economy becomes a participant upon the date of a positive findings report.

**Accountability agents**

The APEC CBPR system uses APEC-recognised accountability agents to review and certify participating organisations’ privacy policies and practices as compliant with the APEC CBPR system requirements, including the APEC Privacy Framework. Applicant organisations may participate in the CBPR system only upon this certification and it is the responsibility of the relevant accountability agent to undertake certification of an applicant organisation’s compliance with the programme requirements. An accountability agent makes no determination as part of the CBPR verification programme regarding whether the applicant organisation complies with domestic legal obligations that may differ from the CBPR system requirements.

APEC CBPR system requirements for accountability agents include:

_a._ being subject to the jurisdiction of a privacy enforcement authority in an APEC economy participating in the CBPR system;

_b._ satisfying the accountability agent recognition criteria;  

_c._ agreeing to use the CBPR intake questionnaire to evaluate applicant organisations (or otherwise demonstrate that proprietary procedures meet the baseline requirements of the CBPR system); and

_d._ completing and signing the signature and contact information form.

 Proposed accountability agents are nominated by an APEC member economy and, following an application and review process by the Joint Oversight Panel, may be approved by the ECSG upon recommendation by the Panel. Any APEC member economy may review the recommendation as to any proposed accountability agent and present objections to the ECSG. Once an application has been approved by the ECSG, the accountability agent is deemed ‘recognised’. Complaints about a recognised accountability agent are reviewed by the Joint Oversight Panel, which has the discretion to request investigative or enforcement assistance from the relevant privacy enforcement authority in the APEC economy where the agent is located.

No accountability agent may have an actual or potential conflict of interest, nor may it provide services to entities it has certified or that have applied for certification. It must


24 See cbprs.blob.core.windows.net/files/Accountability%20Agent%20Recognition%20Criteria.pdf.

25 See cbprs.blob.core.windows.net/files/Signature%20and%20Contact%20Information.pdf.
continue to monitor certified organisations for compliance with the APEC CBPR system standards and must obtain annual attestations regarding this compliance. It must publish its certification standards and must promptly report all newly certified entities, as well as any suspended or terminated entities to the relevant privacy enforcement authorities and the CBPR Secretariat.

Accountability agents can be either public or private entities and may also be a privacy enforcement authority. Under certain circumstances, an APEC economy may designate an accountability agent from another economy.

Accountability agents are responsible for ensuring that any non-compliance is remedied in a timely fashion and reported, if necessary, to relevant enforcement authorities.

If only one accountability agent operates in an APEC economy and it ceases to function as an accountability agent for any reason, then the economy’s participation in the CBPR system will be suspended and all certifications issued by that accountability agent for businesses will be terminated until the economy once again fulfils the requirements for participation and the organisations complete another certification process.

The CBPR system website contains a chart of recognised accountability agents, their contact information, date of recognition, approved APEC economies for certification purposes and links to relevant documents and programme requirements.26

As of July 2018, the CBPR system recognises two accountability agents: TRUSTe and the Japan Institute for Promotion of Digital Economy and Community. TRUSTe is recognised to certify only organisations subject to the jurisdiction of the United States Federal Trade Commission (FTC). The Japan Institute for Promotion of Digital Economy and Community (now called JIPDEC) is recognised to certify organisations under the jurisdiction of the Ministry of Economy, Trade and Industry of the government of Japan.

CBPR system compliance certification for organisations

Only organisations that are subject to the laws of one or more APEC CBPR system-participating economies are eligible for certification regarding personal information transfers between economies.

An organisation that chooses to participate in the CBPR system initiates the process through submission of a self-assessment questionnaire and relevant documentation to an APEC-recognised accountability agent. The accountability agent will then undertake an iterative evaluation process to determine whether the organisation meets the baseline standards of the programme. The accountability agent has sole responsibility for these first two phases of the CBPR system accreditation process (self-assessment and compliance review).

Organisations that are found to be in compliance with the programme requirements will be certified as CBPR-compliant and identified on the CBPR website. As of June 2018, more than 22 organisations have been APEC CBPR certified, all of which are in the United States, with more in various stages of review.27 Certified companies must undergo annual recertification. As more accountability agents are recognised in the economies participating in the CBPR system, the number of certified organisations is expected to grow.

26 See www.cbprs.org/Agents/AgentDetails.aspx.
27 A current list of APEC-certified organisations can be found at https://cbprs.blob.core.windows.net/files/Copy%20of%20APEC%20CBPR%20Compliance%20Directory_June2018%20Update_.xlsx.
Effect of the CBPR on domestic laws and regulations

The CBPR system sets a minimum standard for privacy protection requirements and thus an APEC economy may need to make changes to its domestic laws, regulations and procedures to participate in the programme. With that exception, however, the CBPR system does not otherwise replace or modify any APEC economy’s domestic laws and regulations. Indeed, if the APEC economy’s domestic legal obligations exceed those of the CBPR system, then those laws will continue to apply to their full extent.

PRP system

Because the CBPR system (and the APEC Framework) applies only to data controllers, who remain responsible for the activities conducted by processors on their behalf, APEC member economies and data controllers encouraged the development of a mechanism to help identify qualified and accountable data processors. This led, in 2015, to the APEC PRP programme, which is a mechanism by which data processors can be certified by an accountability agent. This certification can provide assurances to APEC economies and data controllers regarding the quality and compatibility of the processor’s privacy policies and practices. The PRP does not change the allocation of responsibility for the processor’s practices to the data controller and there is no requirement that a controller engage a PRP-recognised processor to comply with the Framework’s accountability principle.

The Joint Oversight Panel of the CBPR administers the PRP program pursuant to the Charter of the APEC Cross-Border Privacy Rules and Privacy Recognition for Processors Systems Joint Oversight Panel and the Protocols of the APEC Joint Oversight Panel with Regard to the Privacy Recognition for Processors System. The rules governing certification and ongoing accountability closely track the CBPR framework, requiring the Joint Oversight Panel to engage in a similar evaluative process (e.g., issuing a findings report) as it does for data controllers pursuant to CBPR rules.

As of July 2018, two APEC countries have joined the PRP system – the United States and Singapore – with more expected to follow.

iii The CPEA

One of the key goals of the Privacy Framework is to facilitate domestic and international efforts to promote and enforce information privacy protections. The Privacy Framework does not establish any central enforcement body, but instead encourages the cooperation of privacy enforcement authorities within the Asia-Pacific region. APEC established the CPEA as a multilateral arrangement to facilitate such interaction. The CPEA became the first mechanism in the Asia-Pacific region to promote cooperative assistance among privacy enforcement authorities.

28 The PRP Purpose and Background Document can be found at cbprs.blob.core.windows.net/files/PRP%20-%20Purpose%20and%20Background.pdf; and the intake questionnaire for processors is at cbprs.blob.core.windows.net/files/PRP%20-%20Intake%20Questionnaire.pdf.
30 https://cbprs.blob.core.windows.net/files/JOP%20Protocols%20for%20PRP.PDF
Among other things, the CPEA promotes voluntary information sharing and enforcement by:

- facilitating information sharing among privacy enforcement authorities within APEC member economies;
- supporting effective cross-border cooperation between privacy enforcement authorities through enforcement matter referrals and parallel or joint enforcement actions; and
- encouraging cooperation and information sharing with enforcement authorities of non-APEC member economies.

The CPEA was endorsed by the APEC ministers in 2009 and commenced in 2010 with five participating economies: Australia, China, Hong Kong China, New Zealand and the United States. Any privacy enforcement authority from any APEC member economy may participate and each economy may have more than one participating privacy enforcement authority. As of July 2018, CPEA participants included over two dozen Privacy Enforcement Authorities from 10 APEC economies.\(^\text{32}\)

Under the CPEA, any privacy enforcement authority may seek assistance from a privacy enforcement authority in another APEC economy by making a request for assistance. The receiving privacy enforcement authority has the discretion to decide whether to provide such assistance.

Participation in the CPEA is a prerequisite to participation by an APEC economy in the CBPR system. As a result, each participating APEC economy must identify an appropriate regulatory authority to serve as the privacy enforcement authority in the CBPR system. That privacy enforcement authority must be ready to review and investigate a CBPR complaint if it cannot be resolved by the certified organisation or the relevant accountability agent, and take whatever enforcement action is necessary and appropriate. As more member economies join the CBPR system, this enforcement responsibility is likely to become more prominent.

### IV INTEROPERABILITY

Given the global nature of personal information flows, APEC’s Data Privacy Subgroup has been involved in collaborative efforts with other international organisations with the goal of improving trust and confidence in the protection of personal information and, ultimately, to enable the associated benefits of electronic commerce to flourish across the APEC region. While privacy regimes such as the APEC Privacy Framework are drafted at the level of principles, there are often very significant differences in the legal and policy implementation of those principles in different economies around the world. In an effort to bridge those differences and find commonality between the two largest privacy systems, in 2012 APEC endorsed participation in a working group to study the interoperability of the APEC and EU data privacy regimes.

In August 2017, the APEC/EU Working Group met to discuss the impact GDPR will have on their undertaking.\(^\text{33}\) These discussions followed the working group’s 2014 release of a document (the Referential) that mapped the CBPR system requirements and rules under


the EU’s former data protection regime, the EU Data Protection Directive. The Referential identified common and divergent elements of both systems to help multinational companies develop global privacy compliance procedures that were compliant with both systems. In its August 2017 meeting, the Working Group agreed to work to develop a new joint work plan to update its previous work in light of GDPR, focusing on mechanisms that can be used to facilitate cross-border data flows and data protection enforcement between the APEC region and the EU.

V THE YEAR IN REVIEW AND OUTLOOK

In February 2018, the Singapore government officially joined the United States (2012), Mexico (2013), Japan (2014), Canada (2015), and South Korea (2017) as an approved APEC economy participating in the APEC CBPR system. This system is growing slowly, as some economies are waiting to see interest from business and some businesses are waiting for member economies to join. With all the North American Free Trade Agreement countries participating, the CBPR system has taken an important step towards an international presence, which may encourage more APEC member economies and business organisations to participate. IBM became the first company to be certified under the APEC CBPR system, in August 2013; it has been joined by nearly two dozen others, including companies with significant international presence, such as Apple, HP and Merck. All these companies were certified by TRUSTe, the sole accountability agent at the time.

TRUSTe became the first recognised accountability agent under the CBPR system on 25 June 2013 and that status was renewed unanimously by the 21 APEC member economies in early 2015. In early 2016, the 21 APEC member economies approved JIPDEC as Japan’s accountability agent. Mexico and Canada have not yet identified their domestic accountability agents.

Following its first enforcement decision under the CBPR against Very Incognito Technologies Inc in June 2016 for misrepresenting its compliance with the CBPR, the FTC continues to bring enforcement actions under APEC. In 2017, the FTC reached settlements with three additional companies – Sentinel Labs, Inc, SpyChatter, Inc and Vir2us, Inc – in actions where the FTC alleged the companies had misrepresented consumers about their participation in the APEC CBPR system. According to the FTC’s allegations, all three companies’ privacy policies misrepresented that the companies either ‘comply with the APEC CBPR’ or ‘abide by the APEC CBPR’. To settle, the companies signed consent agreements that prohibit them from making misrepresentations about their participation, membership or certification in any privacy or security programme sponsored by a government or self-regulatory or standard-setting organisation.

These cases followed the FTC’s announcement in 2016 that it had sent warning letters to 28 companies who claimed compliance with the CBPR despite failing to meet the CBPR requirements. The FTC has brought actions against other companies for similar

misrepresentations in other trans-border programmes, such as the EU–US Safe Harbor Framework and recently under the Privacy Shield programme. The FTC has reminded companies not to mislead consumers about participation in the new EU–US Privacy Shield programme. These new enforcement decisions indicate that the FTC may play a more active role in the future enforcement of the CBPR.

Chapter 4

ARGENTINA

Adrián Lucio Furman, Mercedes de Artaza and Francisco Zappa

I OVERVIEW

Data protection was introduced to the Argentine legal system following the 1994 constitutional reform, with the incorporation of the habeas data procedure. With this constitutional reform, data protection rights in Argentina acquired constitutional protection and, thus, are considered fundamental rights that cannot be suppressed or restricted without sufficient cause.

In October 2000, Congress passed Law No. 25,326 (the Data Protection Law), which focused directly on data protection. The Data Protection Law defined several data protection-related terms and included general principles regarding data collection and storage, outlining the data owner’s rights and setting out the guidelines for the treatment of personal data. It is an omnibus law largely based on the EU Data Protection Directive 95/46 in force at that time, and the subsequent local legislation issued by the European countries (mainly Spain). Moreover, on 30 June 2003, the European Union issued a resolution establishing that Argentina had a level of protection consistent with the protection granted by the Directive with respect to personal data. The issuance of the General Data Protection Regulation (GDPR) might require a reassessment of this recognition.

In 2014, Law No. 26,951 (the Do-Not-Call Law) created the do-not-call registry and expanded the protection of data owner’s rights. This regulation allows the data owner to block contact from companies advertising, selling or giving away products and services. Companies offering products and services by telephonic means must register with the Agency and consult the list of blocked numbers on a monthly basis before engaging in marketing calls.

On 27 September 2017, the Committee of Ministers of the European Council, assessed Argentina’s Data Protection regime and accepted the country’s request to be invited to join the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. As of the date of this publication, the Convention was in process of being internalised to the local legal framework.

1 Adrián Lucio Furman is a partner and Mercedes de Artaza and Francisco Zappa are associates at M&M Bomchil.
2 Section 43, Paragraph 3 of the National Constitution states that, ‘Any person can file this action to obtain access to any data referring to himself or herself, registered in public or private records or databases, intended to supply information; and in the case of false data or discriminatory data, to request the suppression, rectification, confidentiality or updating of the same. The secret nature of the source of journalistic information shall not be impaired.’
3 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.
The Agency of Access to Public Information (the Agency)\(^4\) is the enforcement authority in charge of applying the Data Protection Law and the Do-Not-Call Law. Among other responsibilities, the Agency is in charge of administrating the do-not-call registry, assisting individuals regarding their rights, receiving claims and carrying out inspections of companies to assess their compliance with the Data Protection Law.

II  THE YEAR IN REVIEW

During the early months of 2017, Justice 2020, a governmental initiative for the design of public policies promoted by the Ministry of Justice together with the Data Protection Agency, proposed amendments to the Data Protection Law and the Do Not Call Law. As of 23 July 2018, this draft bill (the Draft) has yet to be submitted to the legislative branch of government.

The Draft defines new data protection-related terms and clarifies other terms defined by the Data Protection Law.

One of its most relevant changes is the scope of application and jurisdiction of the law, which is not currently regulated by the Data Protection Law. If it is passed, this new law will apply exclusively to individuals – in contrast with the Data Protection Law that is also applicable to legal entities – in the following cases: (1) when the person responsible for the treatment is domiciled in Argentina, even if the data treatment takes place abroad; (2) when the person responsible for the data treatment is not based in Argentina but in a place where Argentine legislation applies by virtue of international law; and (3) when the data treatment of data owners that reside in Argentina is performed by an entity with responsibility for data treatment that is not based in Argentina but whose data-treatment activities are related to the offer of goods or services to data owners in Argentina, or to the monitoring of their acts, behaviour or interests.\(^5\)

With this new wording, the Draft specifically recognises that data treatment involving Argentine residents' personal data can occur abroad and grants the same protections as if the treatment had taken place in Argentina.

The Draft also includes new valid ways for obtaining the data owners' consent for the treatment of their personal data,\(^6\) stating that express consent may be granted in writing, orally or through electronic means or any other similar means that technology may offer.

Moreover, the concept of tacit consent\(^7\) is introduced. Tacit consent shall be deemed granted by the data owner when (1) it emerges clearly from the context of the data treatment; (2) the conduct of the data owner is sufficient to demonstrate the existence of the relevant authorisation. The Draft also states that tacit consent is admissible only when the data requested is necessary for the purpose of the collection and the data owner has been informed of his or her rights arising from the law. Tacit consent is not allowed for the treatment of sensitive data.

The Draft, following the principles set out in the Data Protection Law, expressly prohibits the treatment of sensitive data, with the following exceptions: (1) the data owner

---

4 The Agency of Access to Public Information was created by Decree 746 dated 26 September 2017 which amended the Ministries Law No. 26.951.
5 Section 4 of the Draft.
6 Section 12 of the Draft.
7 Section 12 of the Draft.
has granted his or her express consent to the treatment (with the exception of such cases in which, by law, the granting of such consent is not required); (2) the treatment is necessary: to protect the vital interest of the data owner and the latter – or its representatives – are physically or legally unable to provide consent in a timely manner; for the fulfilment of labour and social security obligations in relation to the data treatment itself or to the data owner; for the recognition, exercise or defence of rights in a judicial procedure; for historical, statistical or scientific purposes, in which case dissociation of data must take place; for public health or sanitary assistance; (3) the treatment is carried out by health institutions or professionals, foundations, civil associations of non-profit organisations with political, philosophical, religious or union purposes in connection to their members. The treatment of sensitive data is also allowed when the data has been made public by the data owner.

Following the Regulation (EU) 2016/679 of the European Parliament and of the Council, the Draft expressly addresses and regulates the consent given by children or teenagers for the treatment of their personal data.8 The Draft establishes that such consent shall be deemed valid when it is applied to the processing of data directly linked to information services specifically designed and suitable for children or teenagers. Teenagers can grant their consent from 13 years of age. For children under 13 years old, the treatment of their personal data shall be considered lawful only if consent is granted by the child’s parent or guardian.

Another relevant addition by the Draft is the inclusion of standard procedures and relevant guidelines to be followed by data processors in the event of security and data breaches. In particular, the Draft incorporates the obligation for the person responsible for the data treatment to document and report data incidents to the data owner and the enforcement authority with no delay, and preferably within 72 hours of the acknowledgment of the security breach, unless the breach is unlikely to present a risk to the data owner.9

Regarding the data owner’s rights, 10 the Draft extends the scope of the information to be provided to the data owner when exercising its right of access, stating that the data owner must be informed of not only the existing data and the purposes of its treatment, but also, _inter alia_, (1) the recipients or categories of recipients to whom the personal data has been or will be transferred; (2) the data owner rights, and (3) the existence of automatic decision-making processes, including profiling.

Additionally, the right to data portability is incorporated,11 which establishes that when electronic services that comprise personal data treatment are provided, the data owner will have the right to obtain from the person responsible a copy of the personal data in a structured and commonly used format that allows its subsequent use or its direct transference from responsible entity to responsible entity when it is technically possible.

With respect to users and managers of files, records and databases, specific guidelines related to proactive responsibility are established:12 among the technical and organisational measures to be taken, the person responsible for the treatment should include _inter alia_, internal or external audits, the adoption of a ‘privacy policy’ or the adherence to binding

---

8 Section 18 of the Draft.
9 Section 20 of the Draft.
10 Sections 27 and 28 of the Draft.
11 Section 33 of the Draft.
12 Section 37 of the Draft.
self-regulatory mechanisms to be submitted for approval by the enforcement authority. In particular, it is ordered that measures should be taken to ensure that, by default, only personal data necessary for each of the purposes of the data treatment are processed.

Another relevant addition is the requirement for the creation of a data protection officer, who must be appointed when sensitive data or large-scale data treatment is carried out. The data protection officer’s responsibilities include, inter alia, internal advice and compliance duties in connection to data protection issues.

Binding self-regulating mechanisms are encouraged, and should be filed with the enforcement authority for approval.

The Draft also excludes the possibility of legal entities registering with the do-not-call registry to block contact.

III REGULATORY FRAMEWORK

Privacy and data protection legislation and standards

As expressed above, the Data Protection Law is an omnibus law that regulates data protection in a comprehensive manner. In contrast to other jurisdictions (particularly the United States), Argentina does not have other specific data protection regulations outside the scope of the Data Protection Law, and there is no related legislation at a subnational level.

The Data Protection Law includes principles regarding data protection, data owners’ rights, the organisation of data archives and databases, and actions to protect personal data, to mention a few.

The Law’s main purposes are (1) to protect personal data stored in archives, registers, databanks or other technical means of data processing; (2) to guarantee people’s honour and privacy; and (3) to ensure data owners their rights to access records of their data stored and treated by third parties.

The following are the main principles expressed by the Data Protection Law:

a due registration: data storage will be lawful if the database is duly registered with the Data Protection Agency; and

b data quality: personal data collected must be true, adequate, relevant and not excessive in relation to the scope and purpose for which the data has been obtained. The collection of personal data cannot be done by unfair or fraudulent means. Personal data subject to treatment cannot be used for purposes different from or incompatible with those leading to their collection.

The main rights for data owners contained in the Data Protection Law are the right of information, access and suppression: exercising this information right, data owners can request from the person responsible for the database their personal information that has been collected, the purpose of the collection and the identity of the person responsible for it. Additionally, personal data that is totally or partially inaccurate or incomplete should be deleted and replaced or, if necessary, completed by the file manager when the inaccuracy or incompleteness of the information is known. Data owners do not have to pay to exercise these rights. This right of access can be exercised (1) directly, through the person responsible
for the database; (2) through the Data Protection Agency; or (3) through the habeas data procedure. To guarantee these rights, data must be stored in a way that allows the exercise of the right of access of the owner. Data must be destroyed when it is no longer necessary or relevant for the purposes for which it was collected.

ii General obligations for data handlers

The first obligation for data handlers is to obtain consent from data owners. The treatment of personal data is unlawful when the data subject has not given his or her express consent to the treatment of the data, either in writing or through any other similar means. The consent must appear in a clear and unequivocal manner. There are certain exceptional cases in which consent is not requested, such as when the personal data (1) derives from unrestricted public-access sources; (2) is collected for the performance of public duties; (3) is limited to name, identification card number, tax or social security identification, occupation, date of birth, domicile and telephone number; (4) arises from a contractual relationship and is necessary for the fulfilment of that contract; or (5) refers to the transactions performed by financial entities and arises from the information provided by their customers.

Another important obligation for database owners is the obligation for registration with the Agency. To file the registration, the company or individual responsible for the database must provide information regarding the location of the database, its characteristics and purpose, specifications of the data provided, origin, means of collection, etc. This registration must be renewed annually. The registration process is simple and relatively inexpensive.

iii Specific regulatory areas

The Data Protection Law contains several specific regulations applicable to different areas and industries.

One of the most relevant areas is financial information provided by private registries issuing reports. In that sense, to analyse a prospective client’s financial records it is common for banks and other financial entities to seek credit information through different credit information services.

The Data Protection Law specifies which information can be treated. First, it needs to be personal data of an economic nature and it must be obtained from public sources or have been given by the data owner or collected with the data owner’s consent.

Additionally, information regarding the fulfilment (or not) of a party’s financial obligations can be given by the creditor (or by someone acting on its behalf), since both parties are owners of the information. In this case, there is no need to obtain the other party’s consent.

Information relevant for the assessment of someone’s financial capacity can be stored, registered or transferred for a maximum of five years. If the debtor cancels the debt, or it expires by any means, the period shall be reduced to two years. This issue tends to generate a substantial number of claims from consumers and users of financial services.

The Data Protection Law regulates the treatment of personal data by health institutions too. Public and private hospitals and health professionals can process their patients’ data relating to mental or physical health, as long as they respect professional secrecy. These registries are very useful for scientific purposes, but it is important to note that they store sensitive data and dissociation of data is advised.

Furthermore, security and surveillance industries are also regulated and are currently the focus of most of the inspections carried out by the Data Protection Agency. Disposition
10/2015 regulates the use of closed-circuit television cameras in public spaces. The Disposition establishes that the use of these cameras is lawful when the data handler has obtained the data owner’s prior and informed consent. Consent shall be deemed as granted by the data owner if the data collector includes signs indicating the existence of these cameras, the purpose of the data collection, the person responsible for the treatment and the relevant contact information. A template of this sign is included in the Disposition. The relevant database must be registered and the data collector must implement a manual for its use.

iv Technological innovation

The Data Protection Law has not been amended recently. For that reason, several technological innovations fall outside its scope.

The use of cookies, for example, was not included in the legislation. Nevertheless, by application of the Data Protection principles, companies trying to obtain information through them must obtain the user’s consent to collect information.\(^{15}\)

The use of Big Data, on the other hand, presents a much deeper issue. Through Big Data, companies collect large amounts of information and its different uses are not always clearly determinable since data is often reused – so violating one of the Data Protection Law’s main principles, which is specifying to the data owner the purpose of the data collection. Moreover, data treated must be accurate, true and not excessive in relation to the purpose. In many cases, it is not possible to assess that all information is accurate. Because of the large volume of information provided, some of it is bound to be inaccurate.\(^{16}\) The Data Protection Law has fallen behind in regulating the use of Big Data. The collection of excessive amounts of information is only of benefit to the user, and regulation of Big Data must recognise this new and useful way of treating data and always respect the user’s rights.

The Agency has enacted several regulations aimed at reducing the technological gap generated between the enactment of the Data Protection Law and the present day. For example, Disposition 10/2015 establishes that companies using closed-circuit television cameras must implement a policy that includes the means of data collection, a reference to the place, dates and hours of operation of the cameras, technical and confidentiality mechanisms to be used, ways of exercising the data owner’s rights and, if applicable, reasons that justify obtaining a picture of the individuals entering the facilities.

Moreover, Disposition 18/2015 establishes ‘best practice guidelines for data collection through apps’. In addition to explaining specifically how data protection principles operate in this matter, the Disposition establishes that the privacy policy should be clear and easily accessible for users. Moreover, the privacy policy for apps designed for use on phones or tablets must be shown in a useful way for users, bearing in mind the size restrictions that apply to these devices. The use of icons, pictures, distinctive colours and sounds is recommended; extra care is requested when the app is suitable for children or teenagers.

Lastly, Disposition 20/2015 regulates the collection of photos, films, sounds or any other data in digital format through VANTs or drones.

\(^{15}\) Osvaldo Alfredo Gozaini, Habeas Data, Protection of Personal Data (Rubinzal-Culzoni), p. 325.

\(^{16}\) Luciano Gandola, ‘Conflicts between Big Data and the Data Protection Law’, Infojus.
IV INTERNATIONAL DATA TRANSFER AND DATA LOCALISATION

Every nation that has specifically regulated data protection has realised that any form of planning and controlling would become useless if collected data could be automatically and unrestrictedly transferred abroad to be processed. Following the European model, the Data Protection Law has, in principle, prohibited international data transfer when the transfer is to countries or international or supranational organisations that do not offer ‘adequate levels of protection’.

With this provision, Argentina has tried to avoid data being collected and treated in its territory without regulatory controls in place or without the data owner being able to exercise its rights. Where there are no regulatory controls in place or data owners are unable to exercise their rights, international data transfers are prohibited.

It is considered that a country or organism has an adequate level of protection when that protection derives directly from the legal order, self-regulatory measures or contractual clauses that include specific data protection provisions.

On that basis, Disposition 60 – E/2016 sets forth that the following countries have an adequate level of protection: Member States of the European Union and members of the European Economic Area (EEA), Switzerland, Guernsey, Jersey, Isle of Man, Faroe Islands, Canada (only in relation to its private sector), Andorra, New Zealand, Uruguay and Israel (only in relation to the data handled automatically). International data transfers to countries other than those mentioned above must be made under a standard agreement (similar to the Standard Clauses of the EU). If the parties decide to resort to a different agreement that does not contain the principles, guarantees and content related to the protection of personal data foreseen in the standard clauses, said agreement shall require the approval of the Agency within a 30-calendar-day term as from the date of its execution.

Regulatory Decree 1558/2001 states that if the data owner has given its consent, it does not matter whether the state or organisation does not offer an adequate level of protection and, in that case, the international transfer can take place.

Additionally, consent is not necessary if the personal data is stored in a public registry legally created to provide information and that is open for public consultation or by anyone evidencing a legitimate interest.

The aforementioned prohibition will not apply in cases of (1) international judicial cooperation; (2) transfer of medical information, when the treatment of the deceased requires it, or in the case of an epidemic investigation; (3) bank or stock transfers; (4) transfers decided under international treaties to which Argentina is a party; and (5) when it takes place because of cooperation between agencies fighting organised crime, terrorism or drug trafficking.

V COMPANY POLICIES AND PRACTICES

Although it is not expressly set out in the legislation, companies are encouraged to implement a privacy policy that regulates their personal data collection, treatment and processing and security mechanisms. It is common for the Agency to request this policy from companies upon inspections.

---

17 See footnote 3.
18 Section 12 of the Data Protection Law.
As previously detailed above, Disposition 10/2015 requires companies to draft a manual for the operation of closed circuit television cameras and Disposition 18/2015 contains guidelines for drafting privacy policies for app developers.

**VI DISCOVERY AND DISCLOSURE**

As stated above, data owners have several rights that derive from the Data Protection Law. Nevertheless, the rights of access, rectification and suppression can be denied when they could affect Argentina’s national security, order or public safety, or the protection of rights or interests of third parties.

Additionally, information regarding personal data can be denied when the disclosure of information could become an obstacle to judicial or administrative proceedings regarding tax matters, pension obligations, the development of health and environmental control functions, the investigation of criminal offences or the verification of administrative infringements. The resolution denying access must be reasoned and notified to the affected party, and must relate to the reasons established above.

Since these provisions include a limitation of rights, they should be interpreted restrictively. Additionally, to safeguard the data owner’s rights, this limitation must be subject to judicial review.

Despite all these provisions, the data owner must be able to access the registries if his or her defence rights rely on this action, in which case the access restriction must be lifted.

**VII PUBLIC AND PRIVATE ENFORCEMENT**

**i Enforcement agencies**

The Agency is an autonomous body within the scope of the Chief of Staff. Its main functions in relation to personal data are (1) operating as a registry of databases, keeping records of the registration and renewal of databases; (2) enforcing the Data Protection Law and the Do-Not-Call Law, carrying out inspections and imposing sanctions; and (3) creating new dispositions and regulations related to data protection matters. The Agency is also responsible for assuring the effective exercise of the right of access to public information and the enforcement of transparency within the public sector.

In using these powers, the Agency has issued several dispositions relating to its investigatory and auditing powers. In this context, Disposition 55/2016 regulates the Data Protection Agency’s auditing procedures. The main aims of these proceedings are to control the activity of the person responsible for the database and ensure its compliance with the law.

The proceedings can be (1) *ex officio*, either scheduled annually or spontaneous; or (2) initiated upon a complaint, in which case the inspection itself will have an evidentiary nature.

After the inspection is finalised, the inspector will issue a final report with the outcome of the inspection. If the database owner has complied with the law, the proceeding is finalised. If it has not complied with the regulations, it is granted 15 days to remedy its non-fulfilment, otherwise sanctioning proceedings will begin.

**ii Recent enforcement cases**

The enforcement actions of the Data Protection Agency have evolved and intensified over the years. During its first years, the Agency’s role was more educational than punitive, giving
companies ample time to adapt to the new legislation and being proactive in responding to enquiries and explaining misconceptions. Nowadays, 18 years after the enactment of the Data Protection Law, the Agency is being more proactive in carrying out inspections and is stricter with its enforcement and punitive capabilities.

The vast majority of recent fines have been for violation of the Do-Not-Call Law, resulting in a large number of administrative proceedings and claims. Some fines have also been imposed in the recent past on companies failing to comply with their obligations under the Data Protection Law (mainly failure to register or renew registrations for their databases and failure to comply with security measures).

On a judicial level, most of the case law regarding personal data protection is connected to financial companies and the information they provide to consumer credit reporting agencies regarding their customers’ debts. In most cases, the proceedings relate to financial companies’ failure to update their registries once debts have been paid or the statute of limitations applied.

In this context, the Supreme Court has also stated that the ‘right to be forgotten’ has constitutional rank and must be respected. These cases have all been filed under the habeas data regime.

iii Private litigation

As stated above, the judicial remedy for private plaintiffs is the habeas data procedure regulated by the National Constitution and the Data Protection Law. Despite the fact that the access right of data owners can also be exercised through an administrative procedure, a judicial action is the only way for private plaintiffs to receive financial compensation.

Considering that the administrative procedure before the Data Protection Agency is a fast, free and accessible mechanism, there are not many cases brought at the judicial level. However the Argentine Court of Appeals on Civil Matters has recently issued a valuable decision related to the scope of sensitive data. The case was brought to the judiciary by Instituto Patria, a local institution created by Cristina Fernandez de Kirchner (former president of Argentina) for political purposes, that was fined by the Public Registry of Commerce for its denial to submit its Associates Registry Book in the context of an administrative corporate procedure. Instituto Patria refused to provide such information on the basis that this would constitute a violation to its obligations under the Data Protection Law that prevents the disclosure of sensitive data – in the case related to political orientation – without the consent of the data subject. In turn, the Registry was of the view that the names of the associates could not be deemed as sensitive personal data. The Civil Court of Appeals understood that the names of the associates related to their membership to this organisation were sufficient to reveal their political opinions. Following this approach, it concluded that in this particular case, names could be deemed to be a sensitive personal data. As a consequence, the Court ordered the withdrawal of the Registry’s request and the annulment of the fines applied to Instituto Patria.

---

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

Unlike most recent European legislation and the regulations contained in the Draft, the Data Protection Law does not specifically regulate international jurisdiction. The Agency has no enforcement authority under the current regime regarding companies that are based abroad with no assets or registrations in Argentina, even if these companies collect and treat personal data from Argentine residents. However, foreign companies registered in or that have assets in Argentina must register with the Agency and register their databases, to comply with the Argentine data protection regime.

Consequently, on a theoretical level, what triggers the need to comply with the Argentine regime for personal data protection is the collection or treatment of personal data from Argentine residents. On a practical level, the need to comply with Argentine regulations is triggered by the presence of the foreign company in Argentina by way of assets or registrations in the Public Registry of Commerce.

In 2017, a well-known technology and transport company started offering its services in Argentina, opening offices and hiring personnel. Because of the media coverage its services received, it came to the Agency’s attention that the company was operating through mobile applications that necessarily collected data, but no databases were registered. For that reason, the Data Protection Agency started an investigation and required the foreign company to register its databases with the Data Protection Agency.

IX CYBERSECURITY AND DATA BREACHES

Cybersecurity is not a highly regulated area in Argentina. There are some regulations enacted by the National Central Bank regarding data security obligations for financial institutions, but there is no uniform or omnibus legislation that regulates the matter.

Although Resolution No. 580/2011 of the Chief of Staff created the National Programme for Critical Infrastructures for Information and Cybersecurity, there are not many companies taking part in this programme as it is not mandatory. Its main aim is to promote the creation and adoption of a specific regulatory framework for the protection of strategic infrastructures for the national public sector, inter-jurisdictional organisations and private sector organisations that require it. It seeks the collaboration of those sectors to develop adequate strategies and structures for coordinated action.

Furthermore, Decree 577/2017 has created the Cybersecurity Committee, which will mainly focus on creating a regulatory framework, educating people on the importance of cybersecurity, creating a national cybersecurity plan and creating general guidelines for security breaches. The Ministries of Modernisation, Defence and Security will take part in this initiative.

Resolution General 704-E/2017 of the National Securities Commission dated 29 August 2017 foresees the adoption of international standards with respect to cybersecurity and address the recommendations of the International Organization of Securities Commissions (IOSCO) on the principles of cybersecurity and cybernetic resilience. The Resolution defines the operational risks and deficiencies that might arise related to the processing of data as a consequence of human errors or failures due to external events that might result in the reduction, deterioration or interruption of the services provided by a ‘financial market infrastructure’.
Moreover, Resolution 1107-E/2017 of the Ministry of Defence dated 18 October 2017, created the Security Incident Response Committee that in within the framework of the national cybersecurity plan is responsible for, implementing actions of prevention, detection, response, defines and recovery against cyberthreats within the orbit of the Ministry.

On 26 April 2018, Argentina entered into a memorandum of understanding on cooperation in cybersecurity, cybercrime and cyberdefence between the Argentina and Chile aimed at, inter alia, strengthening the coordination and cooperation, promoting joint initiatives, exchanging good practices, developing and implementing new legislation and national strategies to response to incidents, information exchange, education and training,

Finally, on 27 July 2018, the Agency enacted Resolution 47/18, which contains the recommended security measures for the treatment of personal data through computerised and non-computerised means. Among its dispositions, this resolution recommends data handlers to notify the Agency upon a data breach or security incident.

X OUTLOOK

The future landscape in Argentina regarding personal data protection includes the almost certain enactment of a new law, in line with the new technologies that have emerged since the year 2000.

It is not certain whether the Draft will be sent to Congress and finally passed, but it is the first stepping stone and is certainly one of the Agency’s objectives. We believe that a new law, in line with the GDPR, will be enacted within the next two years. In the meantime, many local companies processing European citizens’ personal data had to adjust their procedures and processing of personal data to the provisions of the GDPR.
I OVERVIEW

The principal legislation protecting privacy in Australia is the federal Privacy Act 1988 (the
Privacy Act). The Privacy Act establishes 13 Australian privacy principles (APPs), which
regulate the handling of personal information by many private sector organisations and by
federal government agencies.

The body responsible for enforcing the Privacy Act is the Office of the Australian
Information Commissioner (OAIC). In practice, the Information Commissioner (the
Commissioner) is responsible for the majority of the privacy-related functions of the OAIC,
including the investigation of complaints made by individuals.

Substantive amendments to the Privacy Act came into effect on 12 March 2014. In
particular, from that date, substantial monetary penalties (currently, up to A$420,000 for
individuals or A$2.1 million for corporations) can now be imposed for ‘serious’ or ‘repeated’
interferences with the privacy of individuals.

Although this chapter is principally concerned with the Privacy Act, each Australian
state and territory has also passed legislation that protects information held about individuals
by state and territory government organisations.

Privacy also receives some protection through developments to the common law,
particularly developments in the law relating to confidential information. However, to
date the Australian courts have not recognised a specific cause of action to protect privacy,
although there has been judicial suggestion that such a development may be open.

There is no general charter of human rights in Australia, and as such there is no general
recognition under Australian law of privacy being a fundamental right.

1 Michael Morris is a partner at Allens.
3 See Australian Broadcasting Corporation v. Lenah Game Meats Pty Ltd (2001) 208 CLR 199.
4 Note, however, that Victoria has enacted the Charter of Human Rights and Responsibilities and the
Australian Capital Territory has enacted the Human Rights Act 2004 (ACT). Both include the right for
individuals not to have their privacy unlawfully or arbitrarily interfered with.
II  THE YEAR IN REVIEW

According to the OAIC’s Annual Report 2016–17 (the most recent report as at 18 July 2018), the OAIC received 2,492 privacy complaints and responded to 16,793 privacy enquiries in the year ending 30 June 2017. The Commissioner also initiated 29 investigations, worked on 14 assessments and received 114 voluntary data breach notifications from organisations.

Although there have been several significant enforcement actions (see Section VII for more information), no monetary penalties have yet been imposed on organisations under the new sanction provisions.

III  REGULATORY FRAMEWORK

i  Privacy and data protection legislation and standards

General

The Privacy Act protects personal information – that is, information or an opinion about an identified individual or an individual who is reasonably identifiable. Special protection is afforded to ‘sensitive information’ (see further discussion below).

The Privacy Act contains exemptions for certain organisations from the requirement to comply with the APPs. Operators of small businesses (businesses with an annual turnover for the previous financial year of A$3 million or less) are not generally subject to the Privacy Act.6 There are also exemptions for domestic use,7 media organisations8 and political representatives.9 There is no general exemption for not-for-profit organisations.

There is a broad exemption10 from the application of the Privacy Act for acts or practices that are directly related to a current or former employment relationship and that involve an employee record held by the employer. In practice, this means that many activities of organisations with respect to their own employees are exempted from the Privacy Act.

There is a limited exemption from the application of the Privacy Act for the sharing of personal information (other than sensitive information) between companies in the same corporate group.11 The rules regarding the disclosure of personal information outside Australia apply even where the information is shared between group companies.

Protection of sensitive information

Sensitive information is defined in Australia as being:

a  information or an opinion about an individual’s:
  •  racial or ethnic origin;
  •  political opinions;
  •  membership of a political association;
  •  religious beliefs or affiliations;

---

6  Section 6D.
7  Section 16 of the Privacy Act.
8  Section 7B(4) of the Privacy Act.
9  Section 7C(1) of the Privacy Act.
10  Section 7B(3) of the Privacy Act.
11  Section 13B of the Privacy Act.
• philosophical beliefs;
• membership of a professional or trade association;
• membership of a trade union;
• sexual orientation or practices; or
• criminal record;

that is also personal information;
b
health information about an individual;
c
genetic information about an individual that is not otherwise health information;
d
biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or
e
biometric templates.

Generally, an organisation must not collect sensitive information about an individual unless
the individual has consented to the collection and the personal information is reasonably
necessary for one or more of the organisation’s functions or activities. An organisation
may collect sensitive information about an individual without consent in certain limited
circumstances; for example, where collection is required by Australian law.

**APP Guidelines (Guidelines)**
The OAIC has published Guidelines to assist organisations in complying with the APPs.
Although the Guidelines are not legally binding, they provide guidance as to how the APPs
will be interpreted and applied by the Commissioner when exercising his or her functions
and powers under the Privacy Act.

**ii General obligations for data handlers**
There is no distinction in the Privacy Act between entities that control and those that process
personal information. Any handling of personal information, whether holding, processing or
otherwise, is potentially subject to the APPs. The 13 APPs are summarised below.

**APP 1 – open and transparent management of personal information**
Organisations must take reasonable steps to implement practices, procedures and systems
that ensure compliance with the APPs. See the discussion on the required content of privacy
policies in Section V.

**APP 2 – anonymity and pseudonymity**
Individuals must have the option of not identifying themselves unless this is impracticable.

**APP 3 – collection of solicited personal information**
Information may be collected only if it is reasonably necessary for the organisation’s functions
or activities and must be collected only by lawful and fair means. An organisation may only
collect information directly from the individual, unless this is unreasonable or impracticable.

**APP 4 – unsolicited personal information**
Where an organisation receives unsolicited personal information, it must, within a reasonable
period, determine whether it could have collected the information itself under the APPs. If
not, the organisation must destroy or ‘de-identify’ that information.
APP 5 – notification of collecting personal information

At or before the time of collection (or as soon as practicable afterwards), an organisation collecting personal information must take such steps (if any) as are reasonable in the circumstances to make the individual aware of a number of prescribed matters; for example:

a. the identity of the organisation;
b. the purposes of the collection;
c. the types of organisation to whom the personal information may be disclosed;
d. whether the organisation is likely to disclose the information to overseas recipients (and, if so, to which countries); and

e. that the organisation’s privacy policy contains certain information (e.g., how to make a complaint).

Where personal information is not collected directly from the individual, an organisation must take reasonable steps to make sure the individual is informed of the same matters in respect of its indirect collection.

APP 6 – uses or disclosures of personal information

Personal information must only be used or disclosed for the purpose for which it was collected (the primary purpose). Personal information may be used or disclosed for a secondary purpose where:

a. the secondary purpose is related to the primary purpose and the individual would reasonably expect it to be disclosed or used this way;
b. the individual has consented to that disclosure or use; or
c. another exception applies (e.g., that the use or disclosure is required by Australian law).

In the case of sensitive information, the secondary use or disclosure under item (a) above must be directly related to the primary purpose.

APP 7 – direct marketing

Sensitive information can only ever be used for direct marketing with the individual’s consent. Other personal information cannot be used or disclosed for direct marketing unless an exception applies. Where direct marketing is permitted, organisations must always provide a means for the individual to ‘opt out’ of direct marketing communications.

APP 7 does not apply to the extent that the Do Not Call Register Act 2006 (Cth) or the Spam Act 2003 (Cth) apply.

APP 8 – cross-border disclosure of personal information

APP 8 regulates the disclosure of information to a person who is outside Australia. See the discussion in Section IV for further details of the requirements of APP 8.

Under Section 16C of the Privacy Act, in certain circumstances, an organisation may be deemed to be liable for a breach of the APPs by an overseas recipient of personal information disclosed by that organisation.
APP 9 – adoption, use or disclosure of government-related identifiers

An organisation must not adopt an identifier that has been assigned to an individual by a government agency as its own identifier of the individual; or disclose or use an identifier assigned to an individual by a government agency, unless an exception applies (e.g., the adoption, disclosure or use is required or authorised by an Australian law).

An identifier includes things such as a driving licence and passport number.

APP 10 – quality of personal information

An organisation must take reasonable steps to ensure that the personal information it collects, uses and discloses is accurate, complete and up to date and also, in the case of use or disclosure, relevant.

APP 11 – security of personal information

Organisations must take reasonable steps to protect information they hold from misuse, interference, loss, unauthorised access, modification or disclosure; and destroy or de-identify information once it is no longer needed for any purpose for which the information may be used or disclosed under the APPs.

APP 11 does not mandate any specific security obligations or standards. The OAIC, however, has published a Guide to securing personal information, which provides non-binding guidance on the reasonable steps organisations are required to take to protect the personal information they hold.

There are no specific rules governing the handling of personal information by third parties. The obligation placed on organisations under APP 11 to take reasonable steps to protect personal information they hold has the effect of requiring organisations to take reasonable steps to ensure that any third party (including an overseas data processor) handling personal information on their behalf also takes reasonable steps to protect personal information. The above-mentioned Guide to information security also provides non-binding guidance in relation to the processing of information by third parties.

APP 12 – access to personal information

As a general rule, an organisation must, upon request, give an individual access to any personal information held about him or her. There are exceptions to this general rule, including where the provision of access to personal information could have an unreasonable impact on the privacy of other individuals, or where denying access is required or authorised by Australian law.

APP 13 – correction of personal information

An organisation must take reasonable steps to correct any personal information if the entity is satisfied the information is inaccurate or where the individual requests the entity to do so. According to the Guidelines, the reasonable steps to be taken may include ‘making appropriate [. . .] deletions’. However, individuals do not have an express legal right to have inaccurate data deleted.

If an organisation refuses to correct personal information, it must give reasons to the person who has requested the correction and tell them about the mechanisms available to complain about the refusal.

### iii Technological innovation and privacy law

The Privacy Act is drafted in a technologically neutral manner and its provisions can be applied to developments in new technologies. As an example, the direct marketing principle, APP 7, has been taken by the Commissioner\(^{13}\) to apply to online behavioural advertising (OBA). In consequence, the requirements of APP 7 (e.g., to allow people to opt out of marketing communications) could apply to advertisements appearing through use of OBA.

As another example, although Australia does not have any specific 'cookie' legislation, the collection of data through the use of cookies could amount to the collection of personal information if the individual’s identity is known or able to be reasonably determined by the collector. In those circumstances, the requirements of the APPs with respect to the information will apply accordingly.

Since sensitive information under the Privacy Act includes biometric information that is used for the purpose of automated biometric identification, it is likely that the use of automated facial and speech recognition technologies will require compliance with the obligations of the APPs relating to sensitive information. Those obligations include the requirement to obtain consent before the relevant biometric information is collected.

### iv Specific regulatory areas

There are a number of state and federal acts that protect privacy in particular circumstances, such as when communicating over a telecommunications network, accessing a computer system, or when engaging in activities in a private setting or that protect specific types of information, such as credit information, tax file numbers, healthcare identifiers, eHealth records or health records.

### IV INTERNATIONAL DATA TRANSFER AND DATA LOCALISATION

APP 8 provides that, prior to disclosing personal information to a recipient who is located outside Australia, an organisation must take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the personal information. This requirement does not apply if:

- the organisation reasonably believes that the overseas recipient is bound by a law similar to the APPs that the individual can enforce;
- the individual consents to the disclosure of the personal information in the particular manner prescribed by APP 8; or
- another exception applies (e.g., that the disclosure of the personal information is required by Australian law).

The consent required by APP 8 has to be an informed consent, and in many cases its requirements are likely to be difficult to satisfy in practice. Further, in many cases the overseas recipient will not be subject to a similar overseas law that is enforceable by the individual. Accordingly, in most cases, the organisation must take ‘reasonable steps’ to ensure that the overseas recipient does not breach the APPs prior to disclosing that information to the overseas recipient. The Guidelines indicate that taking reasonable steps usually involves the organisation obtaining a contractual commitment from the overseas recipient that it will handle the personal information in accordance with the APPs.

V COMPANY POLICIES AND PRACTICES

APP 1.3 requires organisations to have a clearly expressed and up-to-date policy about their management of personal information. An organisation is required to take such steps as are reasonable in the circumstances to make its privacy policy available free of charge and in such a form as is appropriate. This will generally involve the organisation making its privacy policy available on its website.

Aside from the general obligation to include information about the management of personal information, the privacy policy must contain the following specific information:

- the kinds of personal information that the organisation collects and holds;
- how the organisation collects and holds personal information;
- the purposes for which the organisation collects, holds, uses and discloses personal information;
- how an individual may access personal information about the individual that is held by the organisation and seek correction of the information;
- how an individual may complain about a breach of the APPs, or a registered APP code (if any) that binds the organisation and how the organisation will deal with such a complaint;
- whether the organisation is likely to disclose personal information to overseas recipients;
- if the organisation is likely to disclose personal information to overseas recipients, the countries in which such recipients are likely to be located if it is practicable to specify those countries in the policy.

The Commissioner has published in its Guidelines further information as to its expectations with respect to the contents of the privacy policy.

Aside from the specific obligation to have and maintain a privacy policy, APP 1.2 requires an organisation to take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the organisation’s functions or activities that will ensure that the organisation complies with the APPs.

This is an overarching obligation applying to organisations in Australia and is generally understood as requiring organisations in Australia to implement the principles of ‘privacy by design’. Helpful guidance as to what the Commissioner expects organisations to do to comply with this general obligation was published by the Commissioner in May 2015.14

---

VI DISCOVERY AND DISCLOSURE

Under APP 6, in general personal information can only be used and disclosed for the purpose for which the information was collected or for a related secondary purpose that would be reasonably expected by the individual. The disclosure of information in response to national or foreign government requests, or in response to domestic or foreign discovery court orders or internal investigations, would not normally satisfy this requirement. However, there are a number of exceptions that may, depending on the circumstances, be available to allow disclosure in response to such requests or orders. These are summarised below.

In the case of Australian legal proceedings, APP 6.2(b) allows disclosure if the disclosure is ‘required or authorised by or under an Australian law or a court/tribunal order’. This will allow disclosures that are required or authorised under Australian rules of court.

In addition, Section 16A(i)(4) of the Privacy Act allows disclosure where it is ‘reasonably necessary for the establishment, exercise or defence of a legal or equitable claim’. Disclosures of information in the course of legal proceedings where the disclosures are necessary to either assert or defend a claim will accordingly be permitted. Section 16A(i)(5) allows disclosure where it is reasonably necessary for the purposes of a ‘confidential alternative dispute resolution process’. This will permit disclosures in the course of confidential mediations and the like. However, these exceptions do not apply to the disclosure of information to someone outside Australia and so would not be available for claims being pursued in foreign courts.

To disclose information in response to the order of a foreign government or court the disclosure will have to comply with both APP 6 and APP 8 (the cross-border disclosure principle). There has been no binding Australian legal decision on the consequences of a person receiving in Australia an order from a foreign court requiring the disclosure of personal information outside Australia. To satisfy both APP 6 and APP 8, the party seeking disclosure of the information outside Australia is likely to have to apply under a relevant international treaty (such as the Hague Convention), to which Australia is a party and which has been implemented in Australian local law. If these conditions can be satisfied, then the disclosure of the information outside Australia will be ‘required or authorised by or under an Australian law’ and so will be permitted under both APP 6.2(b) and APP 8.2(c).

Another option that might be available in some circumstances would be to redact all personal information from the relevant document before the document is disclosed outside Australia. Whether a document that has been redacted in this way will still comply with the orders of the foreign court will depend on the circumstances.

With respect to disclosures outside Australia, Section 13D(1) provides that acts done outside Australia do not interfere with privacy if the act is required by an applicable law of a foreign country. This exception may be of use where relevant personal information is already located outside Australia and, pursuant to the legal process in the place where it is located, it has to be disclosed to someone in that place. The exception will not be available with respect to information that is located in Australia.

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

If an individual makes a privacy complaint, the Commissioner has the power to attempt, by conciliation, to effect a settlement of the matter or to make a determination that includes declarations that:
the individual is entitled to a specified amount as compensation for loss or damage suffered (including for injury to feelings or for humiliation); 

b the organisation has engaged in conduct constituting an interference with the privacy of an individual and that it must not repeat or continue the conduct; and 

c the organisation perform any reasonable act or course of conduct to redress any loss or damage suffered by the individual.

A determination of the Commissioner regarding an organisation is not binding or conclusive. However, the individual or the Commissioner has the right to commence proceedings in court for an order to enforce the determination.

The Commissioner also has the power to audit organisations (these audits are referred to in the Privacy Act as 'assessments'), accept enforceable undertakings, develop and register binding privacy codes and seek injunctive relief in respect of contraventions of the Privacy Act.

Finally, the Commissioner may apply to the Federal Court or Federal Circuit Court for a penalty (currently, up to A$420,000 for individuals or A$2.1 million for corporations) to be imposed for 'serious' or 'repeated' interferences with privacy. These penalties constitute regulatory fines and cannot be used to compensate individuals for breaches of the Privacy Act. As noted above, the Commissioner has not yet sought to levy the penalty on any organisation.

ii Recent enforcement cases

The Commissioner has recently taken action in a number of significant cases that are of potentially broad interest. These are summarised below.

Enforceable undertaking from Avid Life Media (ALM) following website attack

One of the enforcement powers available to the Commissioner is to accept an enforceable undertaking from an organisation it is investigating for breaches of privacy. Such an undertaking is likely to be offered by the organisation in the course of resolving an investigation by the Commissioner into its activities. The undertakings are enforceable by the Commissioner in the Federal Court.

ALM operates a number of adult dating websites, including ‘Ashley Madison’. It is based in Canada, but its websites have users around the world, including Australia.

In July 2015, a cyber attacker announced the ALM website had been hacked and threatened to expose the personal information of Ashley Madison users unless ALM shut down its controversial website. ALM did not agree to the demand and, as a consequence, information that the hacker claimed was stolen from ALM (including profile information, account information and billing information from approximately 36 million user accounts) was published. This prompted the Commissioner and the Office of the Commissioner of Canada to launch a joint investigation into ALM’s privacy practices.

The OAIC was satisfied that ALM was an organisation with an Australian link as it carried on business and collected personal information in Australia (despite not having a physical presence in Australia). The investigation identified a number of contraventions of the APPs, including with regard to ALM’s practice of indefinite data retention and ALM not having an appropriate information security framework in place.

The Commissioner accepted an enforceable undertaking from ALM to address the concerns identified.


**Provision of an enforceable undertaking by Optus**

On 27 March 2015, the Commissioner accepted an enforceable undertaking from Optus (a major Australian telecommunications company) arising out of its investigation into three privacy incidents involving Optus.

In the first of these incidents, Optus became aware in April 2014 that, because of a coding error, the names, addresses and phone numbers of 122,000 Optus customers were listed in the White Pages directory without those customers’ consent. In the second incident, Optus had issued modems to its customers in such a way that the management ports for the modems were issued with user default names and passwords in place. The consequence was that Optus customers who did not change the default user names and passwords were then vulnerable to a person making and charging calls as though they were the Optus customer. However, there was no evidence that the vulnerability had in fact been exploited. The final incident involved a security flaw that left some Optus customers vulnerable for eight months to ‘spoofing attacks’, under which an unauthorised party could access a customer’s voicemail account.

Following an eight-month investigation, the Commissioner concluded that an enforceable undertaking was the most appropriate regulatory enforcement action in the circumstances. This conclusion was due, in most part, to Optus’ cooperation with the Commissioner and steps it had taken to respond to the Commissioner’s concerns. Under the terms of the undertaking, Optus was required to appoint an independent third party to conduct reviews of the additional security measures Optus adopted in response to the privacy incident and its vulnerability detection processes concerning the security of personal information.

**Metadata collected by telecommunications companies constituted personal information to which the relevant individual could obtain access**

In May 2015, the Commissioner found that metadata could be personal information under the Privacy Act where the organisation holding that data has the capacity and resources to link that information to an individual. The background to that finding was a request made by a journalist to access all metadata that Telstra (Australia’s largest telecommunications company) stored about him in relation to his mobile service. Over the course of some months, Telstra ultimately released much of the requested metadata to the journalist, but continued to refuse access to IP address information, URL information and cell tower location information beyond that which Telstra retained for billing purposes.

The Commissioner found that the above three categories of information did constitute personal information under the Privacy Act and that Telstra had breached the Privacy Act by failing to release that information.

The decision was overturned by the Administrative Appeals Tribunal (AAT) in December 2015. The AAT reasoned that mobile network data would need to be information ‘about an individual’ for it to fall within the definition of personal information. It found that the relevant mobile network data was not information about an individual as such, but rather information about the way in which Telstra delivers its services. It could not, therefore, be characterised as personal information under the Privacy Act and did not need to be disclosed to customers upon request.
In coming to the conclusion that the mobile network data was not personal information, the AAT appears to have been influenced by evidence from Telstra that its mobile network data were kept separate and distinct from customer databases, rarely linked to these databases and not ordered or indexed by reference to particular customers.

On 14 January 2016, having considered the AAT’s decision, the Commissioner filed a notice of appeal from a tribunal to the Federal Court of Australia. The Federal Court dismissed the Commissioner’s appeal on 19 January 2017. In dismissing the appeal, the Court confirmed that if information is not ‘about an individual’, the information will not be personal information and, accordingly, the Privacy Act will not apply.

Enforceable undertaking from the Australian Red Cross following inadvertent disclosure by a third-party contractor

On 5 September 2016, a file containing personal information of approximately 550,000 individuals was inadvertently posted to a publicly accessible section of the Australian Red Cross (the Red Cross) website by a third-party contractor. This included ‘personal details’ and identifying information such as names, gender, addresses and sexual history.

The Red Cross was only made aware of this breach after an unknown individual notified the Red Cross through multiple intermediaries on 25 October 2016. Upon notification, the Red Cross took a number of immediate steps to contain the breach. This included notifying affected individuals, undertaking a risk assessment of the information compromised and conducting a forensic analysis on the exposed server.

The Commissioner found that the Red Cross did not breach the obligation relating to unauthorised disclosure of personal information, as it did not disclose personal information, this was done by a third-party employee. In addition, it was found that although the Red Cross did not physically hold the personal information, it retained ownership of the information because of the terms of its contract with the third-party contractor. Because of its ownership of the personal information, the Red Cross had an obligation to protect this personal information against unauthorised access or disclosure. The Commissioner concluded that the Red Cross had breached this obligation by failing to properly assess the adequacy of its third-party contractor’s security practices and by failing to include control measures to mitigate the risks of contracting with a third party in its contractual arrangements.

The Red Cross accepted an enforceable undertaking on 28 July 2017 to engage an independent review of its third-party management policy and standard operating procedure. The third-party contractor also entered into an enforceable undertaking with the Commissioner’s office to establish a data breach response plan and update its data protection policy.

iii Private litigation

In general, privacy legislation is only enforceable in Australia by the relevant authority. However, some limited private rights of action do exist, particularly a general right under the Privacy Act for anyone to seek an injunction to restrain conduct that would be a contravention of the Act.15

© 2018 Law Business Research Ltd
VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

The Privacy Act has a broad extraterritorial application and applies to the overseas activities of Australian organisations and foreign organisations that have an ‘Australian link’.16

An organisation is considered to have an ‘Australian link’ if there is an organisational link17 – for example, the organisation is a company incorporated in Australia; or if the organisation carries on business in Australia and collects or holds personal information in Australia.18 This has been interpreted very broadly as including an organisation that has a website that offers goods or services to countries including Australia.19

If an organisation’s overseas activity is required by the law of a foreign country, then that activity is not taken to amount to an interference with the privacy of an individual.20

IX CYBERSECURITY AND DATA BREACHES

As stated above, APP 11 requires an organisation to take such steps as are reasonable in the circumstances to protect information from misuse, interference and loss; and from unauthorised access, modification or disclosure.

The obligation in APP 11 would extend to taking reasonable steps to protect information that an organisation holds against cyberattacks. See the discussion on APP 11 in Section III for more details of its requirements.

In addition to the general obligation under APP 11, particular industry sectors are subject by their regulators to take additional measures to protect information (including personal information) that they hold. Government agencies are also generally subject to government-specific security requirements, most notably the Protective Security Policy Framework.

The Privacy Amendment (Notifiable Data Breaches) Act 2017 came into effect on 22 February 2018 and amended the Privacy Act to impose an express obligation on entities to notify the OAIC, affected individuals and at-risk individuals in the event of an ‘eligible data breach’.

An eligible data breach refers to any unauthorised access, disclosure or loss of information that a ‘reasonable person’ is ‘likely’ to conclude would result in serious harm to an individual. In the event an entity becomes aware that an eligible data breach may have occurred, it must provide a copy of a statement to the OAIC setting out the details of the breach as soon as is practicable. It must also subsequently notify any individuals affected by or at risk of being affected by the eligible data breach.

---

16 Section 5B(1A) of the Privacy Act.
17 Section 5B(2) of the Privacy Act.
18 Section 5B(3) of the Privacy Act.
20 Section 13D(1) of the Privacy Act.
X  OUTLOOK

On 31 August 2017, the OAIC released its Corporate Plan 2017–2018.21 The Corporate Plan indicates that the OAIC will focus on the following activities in the coming year: compliance with the new Notifiable Data Breaches scheme; conducting targeted privacy audits (assessments) in areas of national security, national health and identity management to assess organisations’ compliance with the Privacy Act; and the development of an Australian Public Services Privacy Governance Code.

I OVERVIEW

The Belgian legislative and regulatory approach to privacy, data protection and cybersecurity is quite comprehensive. The most important legal provisions can be found in the following:

a the General Data Protection Regulation 2016/679 (GDPR), which is the EU regulation on data protection and privacy;

b Article 22 of the Belgian Constitution, which provides that everyone is entitled to the protection of his or her private and family life;

c the Act of 30 July 2018 on the Protection of Natural Persons with regard to the Processing of Personal Data (the Data Protection Act) (replacing the former Belgian Data Protection Act of 8 December 1992 with effect as of 5 September 2018). It concerns the further implementation of the GDPR and Directive 2016/680 regarding the processing of data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences;

d the Act of 3 December 2017 on the establishment of the Data Protection Authority;

e Book XII (Law of the Electronic Economy) of the Code of Economic Law, as adopted by the Act of 15 December 2013;

f the Act of 13 June 2005 on Electronic Communications (the Electronic Communications Act); and

g the Act of 28 November 2000 on Cybercrime.

Because of a series of cybersecurity attacks on a number of banks and private companies in the past few years, cybersecurity has increasingly received more and more attention in Belgium in recent years. One of Belgium’s most notable cybersecurity incidents, however, was the lightning strike in 2015 at the Google data centre in Mons, which was struck four times during a summer storm, resulting in permanent data loss on a tiny fraction (0.000001 per cent) of the total disk space.

Since presenting its national cybersecurity strategy in 2012, Belgium has made substantial efforts to enhance cybersecurity. For instance, a secret Belgian operation in 2016 prevented the worldwide cyberattacks by the WannaCry ransomware virus from causing large-scale damage in Belgium in 2017. The Centre for Cybersecurity Belgium (CCB) had collected data from the global IT security company Rapid7 on Belgian companies’ cybersecurity in 2016 after the country scored badly in Rapid7’s National Exposure Index report that year, and used this information to warn companies. In 2017, Belgium was ranked...
as the 179th most exposed country of 183 countries, in comparison with 2016, when it was ranked first, and therefore the most exposed country. However, in 2018 Belgium has risen to be the 33rd most exposed country of 187 countries. Belgium scores high due to offering a higher percentage of exposed services in relation to its allocated IP address space. Belgium scores badly for, among other things, having a larger percentage of unencrypted port systems for email access. Cybercrime costs Belgium about €3 billion every year.

Furthermore, while the NotPetya ransomware virus did cause some damage within multinationals in Belgium, the federal cyber-emergency team (CERT) reports that efforts made after the WannaCry ransomware attack have paid off, as the damage in Belgium was limited. The responsibilities of the CCB and CERT are discussed further in Section IX. Belgium is now looking to also improve cybersecurity in the military field, with the Belgian army recruiting 92 computer experts in 2017, and planning to recruit up to 200, to form a ‘cyber-army’ responsible for protecting possible military targets. In addition, the police units want to increase the number of cyberspecialists to 700 by 2030.

II THE YEAR IN REVIEW

The Brussels Court of first instance rendered its judgment on 16 February 2016 in the case against Facebook initiated by the Belgian Privacy Commission (renamed the Data Protection Authority (DPA) on 25 May 2018). This case concerned Facebook’s use of ‘social plug-ins’ to track the internet behaviour of not only its users, but also internet users without a Facebook account. In its judgment, the Court determined that Facebook did not respect Belgian privacy legislation, as it did not provide its customers with sufficient information regarding the data it collected, the purpose thereof, how the data is processed and how long the data was retained. Facebook also did not receive valid consent to collect and process this data. Therefore, Facebook was ordered to stop registering the internet use of people that use the internet from Belgium, until it aligns its policy with Belgian privacy legislation, and must also delete all data that it obtained unlawfully. Facebook has indicated it is disappointed with the judgment, and it has filed for appeal.

Another important judgment, delivered near the end of 2017, related to the ongoing discussion about whether foreign internet service providers, such as Yahoo!, or peer-to-peer internet software providers, such as Skype, are to be considered electronic communications service providers under Belgian law and subject to the jurisdiction of the Belgian courts.

After the final judgment in the Yahoo! case on 1 December 2015, in which the Belgian Supreme Court dismissed an appeal lodged by Yahoo! against the ruling of the Court of Appeal of Antwerp obliging Yahoo! to disclose to the Belgian judicial authorities (despite the fact that Yahoo! had no establishment or personnel in Belgium) the identity of persons who committed fraud via its email service, the Court of First Instance of Mechelen had to rule on Skype’s duty not only to disclose certain information, but also to provide technical assistance for the interception of the content of ‘live’ voice communications. Whereas the obligation to disclose information (and thus jurisdiction) could be located in Belgium in the Yahoo! case on the grounds of the ‘portability’ of information, this reasoning was difficult to apply by analogy to technical assistance that had to be provided in Luxembourg because Skype is a Luxembourg company and has no infrastructure in Belgium, and this would require material acts abroad. Nonetheless, the Court of First Instance imposed a fine of €30,000 on Skype for its refusal to cooperate in setting up a wiretap ordered by the Mechelen investigative judge. The Court ruled that the technical assistance required of Skype was to be extended in
Belgium and the technical impossibility of Skype cooperating was irrelevant because Skype itself had created this impossibility by organising its operations in the way it did. Skype has the duty to make sure it is able to comply with its obligations under Belgian law, and therefore needs to organise itself so it is able to lend its assistance to law enforcement upon request. Skype lodged an appeal against this judgment with the Court of Appeal of Antwerp, which followed the Court of First Instance’s reasoning (see Section VI). Skype has filed for appeal with the Belgian Supreme Court, which is still pending.

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

The Belgian privacy and data protection legislation was set forth in the Data Protection Act, which had to be read in conjunction with the GDPR. However, since the Law of 30 July 2018 entered into force on 5 September 2018, this coexistence has ended.

Belgium had transposed the EU Data Protection Directive quite literally. Its definitions therefore lean closely towards those used in EU law, but must be amended in light of the GDPR. Under the GDPR, ‘personal data’ means any information relating to an identified or identifiable natural person whereby an ‘identifiable person’ is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, 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.

The data controller is the person who alone or jointly with others determines the purposes and means of the processing of personal data, and data processors are persons that process personal data on behalf of a data controller. Under Belgian law, it is also possible for different persons or entities to act as data controller in respect of the same personal data.

The Belgian enforcement agency with responsibility for privacy and data protection is, since the 25 May 2018, the DPA. The old Privacy Commission had as its main mission monitoring compliance and increasing awareness. It could, if needed, also initiate a case before the Belgian courts. The GDPR has broadened the powers of national DPAs, and the Belgian Privacy Commission was consequently reformed into the Belgian DPA in order to reflect this. In accordance with the Act of 3 December 2017, the DPA now has broad investigative powers, and the ability to impose temporary measures as well as administrative fines up until four percent of worldwide turnover.

The Data Protection Act brought to a logical end the peculiar coexistence of the Belgian Data Protection Act of 8 December 1992 with the GDPR. The GDPR came into force on 25 May 2018 and directly applies to data-processing activities performed by Belgium-based controllers and processors. After the Act of 3 December 2017 creating the DPA (replacing the Commission for the Protection of Privacy) tasked with monitoring compliance by Belgian entities with their privacy obligations, the Data Protection Act is the second piece of legislation triggered by the GDPR. The Data Protection Act implementing the GDPR was approved by the parliament on 30 July 2018, and entered into force on 5 September 2018. The Act deals with, among others, areas in the GDPR where the national legislator was able to add additional or clarifying requirements. This includes the age of children’s consent, additional requirements for the processing of genetic, biometric and health data, additional requirements regarding the processing of criminal data, restrictions regarding processing for
journalistic purposes and for the purpose of academic, artistic or literary expression, and additional exceptions for the processing for the purpose for archiving in the public interest or for scientific or historical research or statistical purposes.

The Belgian legislation set 13 as the age from which children may provide consent for the use of an information service, lower than the age of 16 set by the GDPR.

Regarding the processing of genetic, biometric and health data, or data related to criminal convictions and offences, the Belgian legislator has set out measures that must be taken, such as maintaining a list of persons entitled to consult the data, together with a description of their functions, related to the processing of such data, which are bound by a legal or contractual duty of confidentiality. The controller or processor must make a list of these persons available to the DPA on request. Although the latter obligation is not part of the GDPR, it existed previously under the Belgian Data Protection Act of 8 December 1992 and its implementing acts. Where applicable, affected entities must implement the new requirements under the Data Protection Act.

Concerning the processing of criminal data, the Belgian legislator has added additional grounds to process data, similar as those that had already been provided for in the Belgian Data Protection Act of 8 December 1992. As with the processing of genetic, biometric and health data, the persons entitled to consult these data must be designated, bound by a legal or contractual duty of confidentiality, and a list must be kept at the disposal of the DPA. The following are additional grounds for processing of criminal data:

a. by private companies, if necessary for the management of litigation to which the company is a party;
b. by legal advisers if necessary to defend the interests of a client;
c. if necessary for substantial public interest reasons or to perform a task in the public interest; and
d. if necessary for archiving, scientific, historical research or statistical purposes.

The Belgian legislator has also included specific exceptions to data subject rights for processing for journalistic, academic, artistic or literary purposes, as well as for archiving in the public interest or for scientific or historical research or statistical purposes. For journalistic, academic, artistic or literary expression purposes, some of the articles of the GDPR such as consent, information obligation, right to restrict processing and right to object do not apply. It is noteworthy that disclosure of the register, personal data breach notifications and the duty to cooperate with the DPA also does not apply if this would jeopardise an intended publication or constitute a prior control.

Concerning archiving in the public interest or for scientific or historical research or statistical purposes, the data subject’s rights are also restricted if these rights would render it impossible or seriously impair the achievement of these purposes. However, additional requirements are also imposed, such as an explanation in the records of why these data are processed, why an exercise of the data subject’s rights would impair the achievement of the purposes and a justification for the use of data without pseudonymising these data – as well as if necessary a data processing impact assessment. Data subjects should be informed whether the data are pseudonymised, as well as why the exercise of their rights would impair the achievement of the aforementioned purposes.

Belgium-based data controllers and processors should review their data protection documentation (for example, their privacy notices) to update any references to the Belgian Data Protection Act of 8 December 1992.
The new Data Protection Act consolidates the patchy Belgian data protection regulatory framework. For example, it incorporates the provisions of the Act of 25 December 2016 on the processors of passenger data.

In implementing Directive 2016/680 on the processing of personal data by criminal authorities, the Data Protection Act imposes certain requirements on government entities that before were hardly affected by the Belgian Data Protection Act of 8 December 1992. For example, army forces and intelligence and security services must now comply with requests from data subjects to exercise certain data protection rights, albeit in a restricted fashion.

### General obligations for data handlers

Data may be processed if the processing meets one of the following requirements (Article 6 of the GDPR):

- **a** the data subject has unambiguously given his consent to the processing of his or her personal data for one or more specific purposes;
- **b** processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;
- **c** processing is necessary for compliance with a legal obligation to which the controller is subject under or by virtue of an act, decree or ordinance;
- **d** processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- **e** processing is necessary for the performance of a task carried out in the public interest or in the exercise of the official authority vested in the controller; or
- **f** 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 that require protection of personal data, in particular where the data subject is a child.

The processing must comply with the general principles of data processing, which implies that personal data is to be:

- **a** processed fairly and lawfully in a transparent matter;
- **b** collected for specific, explicit and legitimate purposes, and not processed in a manner incompatible with those purposes;
- **c** adequate, relevant and not excessive;
- **d** accurate and, where necessary, up to date;
- **e** kept in an identifiable form for no longer than necessary; and
- **f** processed in a manner that ensures appropriate security of the personal data.

Sensitive personal data (i.e., personal data related to racial or ethnic origin, political opinions, sexual orientation, religious or political beliefs, trade union membership, 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 or judicial information) may only be processed in accordance with the GDPR if the processing:

- **a** is carried out with the data subject's explicit written consent for one or more specified purposes;
b is necessary for a legal obligation in the field of employment, social security and social protection law in as far as it is authorised by law providing for appropriate safeguards for the fundamental rights and interests of the data subject;

c is necessary to protect the vital interests of the data subject where the data subject is unable (physically or legally) to give consent;

d is carried out in the course of its legitimate activities with appropriate safeguards by a non-profit body and relates to members of that body or persons who have regular contact with it and that the personal data are not disclosed outside that body without the consent of the data subjects;

e relates to data manifestly made public by the data subject;

f is necessary for legal claims;

gh is necessary for reasons of substantial public interest, which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

i is necessary for medical reasons;

j is necessary for reasons of public interest in the area of public health on the basis of law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy; or

Regarding consent, it must be added that parental consent is required for the processing of personal data concerning information services for children under the age of 13 (as opposed to the age of 16 in Article 8.1 of the GDPR).

As mentioned before, the new Data Protection Act also further regulates possible exceptions regarding the processing of the above special categories of data in implementation of the GDPR.

In practice, however, the ground of legitimate interest is frequently relied upon (rather than consent) as a ground for processing non-sensitive personal data. It should be noted, however, that the DPA finds that obtaining the unambiguous consent of the data subject is best practice and that the legitimate interest condition is only a residual ground for processing.

Except with respect to the processing of sensitive personal data, where consent of the data subject must be provided in writing, Belgian law does not impose any formalities regarding obtaining consent to process personal data. Such consent may be express or implied, written or oral, provided it is freely given, specific and informed. However, as consent should be unambiguous as well, it is recommended to obtain express and written consent for evidential purposes.

With respect to the processing of employees’ personal data, the DPA finds that such processing should be based on legal grounds other than consent, in particular the performance of a contract with the data subject, since obtaining valid consent from employees is considered difficult (if not impossible) given their subordinate relationship with the employer.

As far as the data subjects’ right of access, correction and removal is concerned, the GDPR provides that a data controller must provide a data subject access to his or her data
upon request. The data subject has the right to have inaccurate data corrected or deleted and, in certain cases, he or she may object to decisions being made about him or her based solely on automatic processing.

Since the GDPR is in effect, data controllers no longer need to notify the DPA of all types of data processing operations. Instead, they are bound to keep records of their processing activities. It is now up to the controller to be able to prove that it has obtained consent for its data processing or has a legitimate reason for doing so under the GDPR.

The DPA has issued a recommendation regarding data processing records to be held in 2017. In this recommendation, the DPA explains that both the controller and the processor must keep records, regardless of whether they are natural or legal persons, or if they are entities without legal personality. These records must be made available upon first request. Exceptions can be made, but these are not absolute. For small entities, the DPA recommends that records are held in any case, even if they would fall under an exception. The DPA, however, does not object to the fact that the records do not include occasional, incidental processing of data. The recommendation further includes additional information regarding the Records, such as how it relates to the previous notifications, how these notifications can be used as a starting point for establishing the records, and how the records require a broader registration of data processing that the old notifications did. Old notifications will remain available online for one year after the entry into effect of the GDPR on 25 May 2018. The records can be held in any language, but the DPA may request the data controller or processor to provide them with a translation in one of the national languages. Therefore, if possible, it is advised to keep the records in Dutch, French or German in order to avoid additional costs.

A new obligation under the GDPR is also the appointment of a data protection officer (DPO) in specific cases, such as for public authorities, or when there is large-scale systematic monitoring of personal data or large-scale processing of sensitive data. On 24 May 2017, the DPA issued a recommendation to help data controllers and data processors with the preparation for the implementation of the obligations under the GDPR.

The DPO is not a new concept, as the Directive 95/46/EG did already provide for member states to foresee in a similar non-obligatory function, the appointment whereof would exempt the data controller from making a mandatory notification. In the former Data Protection Act of 1992, however, this function was not linked to an exemption of the notification, but rather an additional requirement that could be imposed by Royal Decree for situations where deemed necessary. A general Royal Decree was never issued in this regard, but specific legislation (such as for specific public databases, the police, and hospitals) did foresee in a mandatory appointment of a person with such a function.

Under the legislation pre-dating the GDPR, the ‘old’ DPO had a more limited function and mostly provided its institution or company with advice regarding compliance. Under the GDPR, the DPO has a much more prominent role, and the DPA considers them to be the cornerstone of accountability. For this reason, the DPA wishes to distance itself from its older advice regarding this function, and emphasises that under the GDPR, the appointment of the appropriate person as a DPO must be investigated separately. In this regard, the appointment of a DPO for government agencies has been reiterated and further regulated in the Data Protection Act.
iii Specific regulatory areas

Although Belgium has not adopted a sectoral approach towards data protection legislation, there are nevertheless separate regulations in place for certain industries and special (more vulnerable) data subjects. In addition to the Data Protection Act, specific laws have been adopted to provide additional protection for data subjects in the following sectors:

a camera surveillance: the installation and use of surveillance cameras is governed by the Camera Surveillance Law of 21 March 2007, which was most recently amended by the Act of 16 April 2018, in order to comply with the GDPR, with the amended provisions taking effect on 25 May 2018, the date that the GDPR entered into effect;

b workplace privacy: the installation and use of surveillance cameras for the specific purpose of monitoring employees is subject to Collective Bargaining Agreement No. 68 of 16 June 1998 concerning the camera surveillance of employees. In addition, the monitoring of employees’ online communication is subject to the rules laid down in Collective Bargaining Agreement No. 81 of 26 April 2002 concerning the monitoring of electronic communications of employees.

c electronic communications: the Electronic Communications Act of 13 June 2005 contains provisions on the secrecy of electronic communications and the protection of privacy in relation to such communications. Furthermore, the Electronic Communications Act imposes requirements on providers of telecommunication and internet services regarding data retention, the use of location data and the notification of data security breaches;

d medical privacy: the Patient Rights Act of 22 August 2002 governs, inter alia, the use of patients’ data and the information that patients need to receive in this respect; and

e financial privacy: the financial sector is heavily regulated. For instance, the use of credit card information for profiling violates consumer credit legislation, which clearly states that (1) personal data collected by financial institutions can only be processed for specific purposes, (2) only some data can be collected, and (3) it is prohibited to use the data collected within the credit relationship for direct marketing or prospection purposes. Belgian legislation also requires that information be deleted when its retention is no longer justified.

Noteworthy in an EU context is the fact that jointly with the entry into force of the GDPR, the Network and Information Security Directive (the NIS Directive) should have been transposed into national law by the EU Member States by 25 May 2018. In addition to the specific data protection rules above, the NIS Directive adds a legal basis for higher cybersecurity standards in respect of certain ‘essential’ services. The Belgian implementation of the NIS Directive is currently still being drafted. The Belgian government has finalised its draft Act, and it is expected that this will soon be presented to the parliament for approval.

Currently, the draft Act will appoint authorised government entities on two different levels, and with separate functions. A national public entity will be charged with monitoring compliance and coordination of the implementation of this Act. On a sectoral level, sectoral authorities will be charged with monitoring compliance for their respective sectors.

The NIS Directive applies in particular to operators of essential services (OESs). OESs can be found in the following industries:

a energy (electricity, oil and gas);

b transportation (air, rail, water and road);

c banking and financial market infrastructure;
To ensure an adequate level of network and information security in these sectors and to prevent, handle and respond to incidents affecting networks and information systems, the NIS Directive sets out the following obligations for these OESs:

- the obligation to take appropriate technical and organisational measures to manage the risks posed to their network and information systems, and to prevent or minimise the impact in the event of a data breach; and
- the obligation to notify the competent authority, without undue delay, of all incidents with a ‘significant impact’ on the security of the core services provided by these operators. To assess the impact of an incident, the following criteria should be taken into account: (1) the number of users affected; (2) the duration of the incident; (3) the geographical spread with regard to the area affected by the incident; and (4) in relation to certain OESs, the disruption of the functioning of the service and the extent of the impact on economic and societal activities.

The notification obligations, preventive actions and sanctions under the NIS Directive should increase transparency regarding network and information security and heighten awareness of cybersecurity risks in the above-mentioned essential services.

The Draft Act foresees in the identification of OES and establishes the safety requirements both on a national and sectoral level, as well as how this is monitored through internal and external audits, and sanctions for non-compliance.

Concerning computer security incidents, computer security incident response teams are established on a national and sectoral level, as well as the procedures regarding the reporting of safety incidents.

### iv Technological innovation and privacy law

#### Big-data analytics

The DPA released in March 2017 a report on the use of big data, on which stakeholders could comment until 11 April 2017.

The report aims to reconcile the need for legal certainty with the application of big data in current and future applications, especially in the light of the GDPR. The recommendations made in the report cover various aspects, such as data protection compliance and respect for data subjects’ rights. It is not the intention of the DPA to curtail unnecessarily the use of big-data applications as they are often very useful to society.

#### Cookies

The use of cookies is regulated by Article 129 of the Electronic Communications Act. This must be read in conjunction with the GDPR, which in Article 30 clarifies that if cookies can be used to identify the user, this constitutes a processing of personal data. The latest amendment to the Electronic Communications Act provides, in line with the requirements of the GDPR, that cookies may only be used with the prior explicit consent of the data subject (i.e., opt-in rather than opt-out consent), who must be informed of the purposes of the use of the cookies as well as his or her rights under the GDPR and the Data Protection Act. The consent requirement does not apply to cookies that are strictly necessary for a service requested by an individual. The user must be allowed to withdraw consent free of charge.
On 4 February 2015, the DPA issued an additional draft recommendation on the use of cookies in which it provided further guidance regarding the type of information that needs to be provided and the manner in which consent should be obtained. This requires an affirmative action by the user, who must have a chance to review the cookie policy beforehand. This policy must detail each category of cookie with their purposes, the categories of information stored, the retention period, how to delete them and any disclosure of information to third parties.

According to the DPA, consent cannot be considered validly given by ticking a box in the browser settings.

In January 2017, the European Commission published the draft text of the new e-Privacy Regulation, which will become directly applicable in Belgium and replace all the current national rules relating to, *inter alia*, cookies after its adoption. Both the European Parliament and the Council have published their respective drafts. The three EU entities are now in the middle of their ‘trilogue’ negotiations to determine the final text. The current draft Regulation would possibly allow consent to be given through browser settings provided that this consent entails a clear affirmative action from the end user of terminal equipment to signify his or her freely given, specific, informed and unambiguous consent to the storage and access of third-party tracking cookies in and from the terminal equipment. This entails that internet browser providers will have to significantly change the way their browsers function for consent to be validly given via browser settings.

In addition, the proposal clarifies that no consent has to be obtained for non-privacy-intrusive cookies that improve the internet experience (e.g., shopping-cart history) or cookies used by a website to count the number of visitors. It was initially foreseen that the e-Privacy Regulation would enter into force simultaneously with the GDPR, but the negotiations have been postponed. The finalisation of the Regulation is foreseen in 2019, after which (much like the GDPR) a transitory period will most likely be foreseen before the Regulation becomes enforceable.

**Electronic marketing**


The automated sending of marketing communications by telephone without human intervention or by fax is prohibited without prior consent.

When a company wants to contact an individual personally by phone (i.e., in a non-automated manner) for marketing purposes, it should first check whether the individual is on the ‘do-not-call-me’ list of the non-profit organisation DNCM. Telecom operators should inform their users about this list and the option to register online. If the individual is registered on the list, the company should obtain the individual’s specific consent before contacting him or her.

Furthermore, the proposal for the new e-Privacy Regulation (already referred to above) in the context of cookie rules) obliges marketing callers to always display their phone number or use a special prefix that indicates a marketing call. Again, as this is only a draft text, it is not certain that this obligation will effectively be imposed on marketing callers.
Likewise, the use of emails for advertising purposes is prohibited without the prior, free, specific and informed consent of the addressee pursuant to Section XII.13 of the Code of Economic Law. This consent can be revoked at any time, without any justification or any cost for the addressee. The sender must clearly inform the addressee of its right to refuse the receipt of any future email advertisements and on how to exercise this right using electronic means. The sender must also be able to prove that the addressee requested the receipt of electronic advertising. The sending of direct marketing emails does not require consent if they are sent to a legal entity using ‘impersonal’ electronic contact details (e.g., info@company.be) which also do not fall within the scope of the GDPR. The use of addresses such as john.doe@company.be, which include personal data, however, remains subject to the requirement for prior consent.

Other exceptions could also apply regarding electronic advertisements, such as for existing clients to whom advertisements are sent for similar products or services, given that the client did not object thereto. These exceptions are based on national legislation predating the GDPR, however. It remains to be seen how the DPA will continue to interpret these exceptions after 25 May 2018, and whether it believes they comply with the strict criteria for processing data under the GDPR. We believe it is likely this will remain the case, as the DPA may accept that they fall under the ‘legitimate interest’ category, for which it has in the past already accepted that the maintenance of customer relationships could provide a legitimate interest.

Unless individuals have opted out, direct marketing communications through alternative means are allowed. Nonetheless, the GDPR prescribes a general obligation for data controllers to offer data subjects the right to opt out of the processing of their personal data for direct marketing purposes.

**Camera surveillance**

On 16 April 2018, the Camera Surveillance Act was amended, both regarding use by law enforcement and use outside of law enforcement. The changes entered into effect on the 25th of May 2018, the same day that the GDPR entered into force. The changes reflect the changes to privacy law brought forward by the GDPR. To install camera surveillance, it is now required that the police, rather than the DPA, be informed. This will take place via an online application.

The data controller will also need to keep a separate record concerning the processing of these data. Further details on this record will be determined by Royal Decree.

It is also required for data controllers who install a surveillance camera in ‘publicly accessible venues’ to indicate the existence thereof with a visible sign in proximity of the camera, as well as the provision in proximity of the camera of a screen that displays the images being recorded.

Regarding the scope of the Camera Surveillance Law, a surveillance camera falling within the scope of this Act is: a fixed (temporarily or permanent) or mobile observation system, with as purpose to survey and guard certain areas which processes images for this purpose.

The purpose is further elaborated in Article 3 of the Camera Surveillance Law as being either of the following:

- prevention, ascertaining or investigation of crimes against persons or goods; or

© 2018 Law Business Research Ltd
Belgium

... prevention, ascertaining or investigation of nuisance in accordance with Article 135 of the New Act on Municipalities, monitoring of the compliance with municipal regulations and public order.

The use of surveillance camera’s regulated by other special legislation or by public authorities does not fall within the scope of the Camera Surveillance Law. If surveillance cameras are used merely to monitor the safety, health, protection of the assets of the company and monitoring of the production process and the labour by the employee, the Camera Surveillance Law is not applicable. However, if the surveillance camera’s would also be used with as purpose one of the purposes listen above in accordance with Article 3 of the Camera Surveillance Law, the Camera Surveillance Law will apply and precede any other legislation.

**Employee monitoring**

Employee monitoring is strictly regulated under Belgian law. Apart from the rules embedded in the Camera Surveillance Act of 16 April 2018, which will apply if the surveillance of employees would fall within its scope as discussed above, the monitoring of employees by means of surveillance cameras in particular is subject to the provisions of Collective Bargaining Agreement No. 68 of 16 June 1998. Pursuant to this Agreement, surveillance cameras are only allowed in the workplace for specific purposes:

- the protection of health and safety;
- the protection of the company's assets;
- control of the production process; and
- control of the work performed by employees.

In the latter case, monitoring may only be on a temporary basis. Employees must also be adequately informed of the purposes and the timing of the monitoring.

With respect to monitoring of emails and internet use, Collective Bargaining Agreement No. 81 of 26 April 2002 imposes strict conditions. Monitoring cannot be carried out systematically and on an individual basis. A monitoring system of emails and internet use should be general and collective, which means that it may not enable the identification of individual employees. The employer is only allowed to proceed with the identification of the employees concerned if the collective monitoring has unveiled an issue that could bring damage to the company or threaten the company's interests or the security of its IT infrastructure. If the issue only relates to a violation of the internal (internet) policies or the code of conduct, identification is only allowed after the employees have been informed of the fact that irregularities have been uncovered and that identification will take place if irregularities occur again in the future. In 2012, the DPA issued a specific recommendation on workplace cyber-surveillance. In this regard, the DPA advises employers to encourage employees to label their private emails as ‘personal’ or to save their personal emails in a folder marked as private. Furthermore, companies should appoint a neutral party to review a former or absent employee’s emails and assess whether certain emails are of a professional nature and should be communicated to the employer.

Finally, GPS monitoring in company cars is only allowed under Belgian law with respect to the use of the company car for professional reasons. Private use of the company car (i.e., journeys to and from the workplace and use during private time) cannot be monitored.
IV INTERNATIONAL DATA TRANSFER AND DATA LOCALISATION

Cross-border data transfers within the EEA or to countries that are considered to provide adequate data protection in accordance with EU and Belgian law are permitted. Transfers to other countries are only allowed if the transferor guarantees that adequate safeguards are in place. This can be done by entering into a model data transfer agreement (based on the EU standard contractual clauses) with the recipient or if the transfer is subject to binding corporate rules (BCRs).

Some countries are deemed to be adequate by the European Commission, such as Switzerland, Canada, Andorra and the United States if the transfer of data meets the requirements as adopted in the EU–US Privacy Shield, Argentina, etc. Recently, an agreement was made between the European Union and Japan. It remains to be seen whether or not the EU–US Privacy Shield will survive the second annual review, or be suspended following the adoption by the US of the Cloud Act allowing police to access personal data outside US boundaries and continuing failure by the US to comply with the Privacy Shield requirements (e.g., the appointment of an ombudsman).

If an international data transfer is concluded under the EU standard contract clauses, a copy of these must be submitted to the DPA for information. The DPA will check their compliance with the standard contractual clauses and will subsequently inform the data controller whether the transfer is permitted. Data controllers need to wait for this confirmation from the DPA before initiating their international data transfer.

In the case of non-standard ad hoc data transfer agreements, the DPA will examine whether the data transfer agreement provides adequate safeguards for the international data transfer. If the DPA believes that the safeguards are adequate, it will forward the request to the European Data Protection Board, which must also approve.

If a data controller gives ‘sufficient guarantees’ for adequate data protection by adopting BCRs, a copy of the BCRs also needs to be sent to the DPA for approval, as well as the European Data Protection Board.

As an exemption to the above, transfers to countries not providing adequate protection are also allowed if the transfer:

a is made with the data subject’s consent;

b is necessary for the performance of a contract with, or in the interests of, the data subject;

c is necessary or legally required on important public interest grounds or for legal claims;

d is necessary to protect the vital interests of the data subject; or

e is made from a public register.

V COMPANY POLICIES AND PRACTICES

Although companies are not explicitly required under Belgian law to have online privacy policies and internal employee privacy policies, in practice they need to have such policies in place. This results from the obligation, under Belgian data protection law, for data controllers to inform data subjects of the processing of their personal data (including the types of data processed, the purposes of the processing, the recipients of the data, the retention term, information on any data transfers abroad, etc.). As a result, nearly all company websites contain the required information in the form of an online privacy policy.

Likewise, companies often have a separate internal privacy policy for their employees, informing the latter of the processing of their personal data for HR or other purposes. Such
a policy sometimes also includes rules on email and internet use. Some companies include the privacy and data protection information in their work regulations. This is the document that each company must have by law and that sets out the respective rights and obligations of workers and employers. The work regulations also provide workers with information about how the company or institution employing them works and how work is organised.

The appointment of a chief privacy officer is not very common in Belgium, except within large (and mostly multinational) corporations. Such corporations often also have regional privacy officers. In smaller companies, the appointment of a chief privacy officer is rare. However, given the increasing importance of privacy and data security, even smaller companies often have employees at management level in charge of data privacy compliance (often combined with other tasks). Of course, with the GDPR, this will become different as for many companies it will now be required to appoint a Data Protection Officer (see above).

The GDPR contains an obligation to conduct a data protection impact assessment (DPIA) for high-risk data processing activities. The DPA has taken the liberty of issuing recommendations on the DPIA requirement of the GDPR. In addition to the non-exhaustive list of processing activities as envisaged by the GDPR (i.e., any processing that entails a systematic and extensive evaluation of personal aspects that produce legal effects; any processing on a large scale of special categories of data; and any systematic monitoring of a publicly accessible area on a large scale), the DPA clarifies its position on what qualifies as high risk, when a DPIA must be conducted, what it should entail and when it should be notified of the results of a DPIA. The main takeaway of the DPA’s statement is that it should only be notified of processing activities where the residual risk (i.e., the risk after mitigating measures have been taken by the controller) remains high. Whether the DPA’s position will be supported at EU level remains to be seen, since the interpretation of DPIA methodologies is in principle an EU-level matter.

A substantial number of companies have conducted privacy audits certainly now in view of the implementation of the GDPR to get a clear view on their data flows and security measures. These audits have often resulted in the implementation of overall privacy compliance projects, including the review and update of IT infrastructure, the conclusion of data transfer agreements or adoption of BCRs and the review and update of existing data processing agreements with third parties.

In large organisations, it is considered best practice to have written information security plans. Although this is also not required by law, it proves very useful, as companies are required to present a list of existing security measures when they notify their data processing operations to the DPA. The DPA has also recommended that companies have appropriate information security policies to avoid or address data security incidents. This has become even more important now in view of the short deadlines for data breach notifications under the GDPR.

On 14 June 2017, the DPA published a recommendation on processing-activity record-keeping as discussed above. As from the entry into force of the GDPR in 2018, organisations processing personal data within the EU must maintain Records of their processing activities. Organisations with fewer than 250 employees are exempted from keeping such records, unless their processing activities:

a are likely to result in a risk to the rights and freedoms of data subjects (e.g., automated decision-making);

b are not occasional; or

c include sensitive data.
On the basis of the above-mentioned non-cumulative conditions, it may be expected that basically all organisations processing personal data will have to maintain records of their processing activities in practice, even if they employ fewer than 250 people. The DPA advises all companies to do so.

In substance, these records should contain information on who processes personal data, what data is processed and why, where, how and for how long data is processed.

VI DISCOVERY AND DISCLOSURE

Pursuant to the Belgian Code of Criminal Procedure, the public prosecutors and the examining magistrates have the power to request the disclosure of personal data of users of electronic communications services (including telephone, email and internet) in the context of criminal investigations. Examining magistrates may also request technical cooperation of providers of electronic communications service providers and network operators in connection with wiretaps.

The personal and territorial scope of application of these powers is currently the subject of a heated debate before the Belgian Supreme Court and criminal courts. In 2009, Yahoo! was prosecuted for non-compliance with the provisions of the Code of Criminal Procedure, as it had refused to disclose certain personal data related to a Yahoo! account that had been used in connection with a drug-related criminal offence. In addition, Skype was also charged with non-compliance as a result of its alleged lack of technical cooperation in connection with a wiretap on the communication of one of its Belgian users (see also Section II). The discussion in both cases deals with two issues: first, can Yahoo!, Skype and similar service or software providers be considered as providers of electronic communications services under Belgian law; and second, does the duty of cooperation set forth in the Belgian Code of Criminal Procedure apply to foreign entities that have no physical presence (no offices, infrastructure, servers, etc.) in Belgium – and if so, can it be enforced against them by the Belgian courts?

A detailed discussion of both questions is beyond the scope of this chapter, but it is interesting to note that the Supreme Court has already issued two surprising decisions in the Yahoo! case that may have far-reaching consequences. In its first decision, the Court has extended the scope of the definition of providers of electronic communications services, so that it includes not only service providers that take care of the transmission of signals and data over the electronic communications networks, but also ‘anyone offering a service that allows its customers to obtain, receive or spread information via an electronic communications network’. This new definition seems problematic for multiple reasons. First, the Supreme Court disregards the very clear definition of ‘providers of electronic communications services’ set forth in the Act of 13 June 2005 on electronic communications. Second, its own definition is very vague and gives courts a great margin of appreciation, which goes against the principle of legal certainty (in particular in criminal matters). Therefore, it can be expected that in the future, the duty to disclose personal data will apply not only to traditional internet access providers and telephone companies, but also to a wide variety of online software or service providers. This broad definition has, after the Supreme Court judgement, now been adopted into the Belgian Code of Criminal Procedure (e.g., in Articles 46 bis, 88 bis and 90 quater of the Code of Criminal Procedure) and is, therefore, indisputable.

The second decision of the Supreme Court in the Yahoo! case is even more important from an international perspective: the Court ruled that even though Yahoo! had no physical presence in Belgium, the provisions of the Code of Criminal Procedure applied to it, as
the ‘service’ it offers can be used in Belgium via the internet. It also stated that the fact
that the public prosecutor sent the request to disclose personal data directly to Yahoo! in
the United States (without making use of the procedures set out in the applicable treaties
regarding mutual legal assistance in criminal matters) did not make the request invalid or
unenforceable.

This latter decision essentially implies that foreign entities offering an online service
(or software) are subject to Belgian criminal law as soon as the software service can be
used in Belgium, and that the Belgian public prosecutor has the power to enforce Belgian
criminal law against such foreign entities without the intervention or assistance of the judicial
authorities of the state of residence of these entities. Obviously, this position taken by the
Supreme Court would also imply that foreign judicial authorities could enforce their national
criminal law against service providers located in Belgium and do so without assistance from
the Belgian courts.

Finally, on 1 December 2015, the Supreme Court put an end to the legal proceedings
by rejecting the appeal, thereby confirming the Court of Appeal’s decision, which has caused
important implications for the international system of mutual legal assistance in criminal
matters.

Analogously, the Court of First Instance of Mechelen condemned Skype
Communications SARL, a Luxembourg-based entity, for refusing to set up a wiretap in
Mechelen in its ruling of 27 October 2016. The wiretap concerned was ordered by the
Mechelen examining judge in the framework of an investigation into a Skype user. Again,
the Belgian authorities ignored the European Convention on Mutual Assistance in Criminal
Matters and imposed the wiretap order directly on Skype in Luxembourg. The Court of
Mechelen applied a similar reasoning to that applied by the Supreme Court in the Yahoo!
case and held that the alleged offence, namely the refusal to provide technical assistance, can
be deemed to have occurred in the place where the information should have been received,
regardless of where the operator was established.

Notably, the context of the Skype case is quite different from the situation in the Yahoo!
case. While the Yahoo! case involved the mere refusal to disclose information to the Belgian
authorities (Section 46 bis Section 1 of the Belgian Code of Criminal Procedure), the Skype
case concerns the provision of metadata and the refusal to set up a wiretap (Article 88 bis
Section 2 and Article 90 quater Section 2 of the Belgian Code of Criminal Procedure).
The latter is undeniably a completely different type of measure, encompassing not only
the provision of information, but also material acts by Skype and the necessary technical
infrastructure to perform them, which Skype did not have in Belgium. Unsurprisingly, Skype
appealed against this judgment before the Court of Appeal of Antwerp, but the Court of
Appeal confirmed the judgment by the Court of First Instance of Mechelen. Notably, the
Court confirmed the fact that Skype has the duty to make sure it has the necessary technical
infrastructure to perform the measures requested (the wiretap), even if this would result in
a large cost for Skype. Skype appealed against this judgment before the Belgian Supreme
Court. This appeal is currently still pending.

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies
The Belgian enforcement agency with responsibility for privacy and data protection is the
DPA.
The DPA’s mission is, *inter alia*, to monitor compliance with the provisions of the GDPR and the Data Protection Act. To this end, the DPA has general power of investigation with respect to any type of processing of personal data and may file a criminal complaint with the public prosecutor. It may also institute a civil action before the president of the court of first instance. Whereas this is where the scope of authority ended for the original Privacy Commission, the reformed DPA (in light of the GDPR) is an independent administrative authority with legal personality and extensive investigative and sanctioning powers, composed of six different bodies: an executive committee, a general secretariat, a front-line service, a knowledge centre, an inspection service and a dispute chamber.

The executive committee, composed of the leaders of the five other bodies, is responsible for the adoption of the DPA’s general policies and strategic plan.

A general secretariat is responsible for the reception and processing of complaints and to inform citizens about their data protection rights.

The inspection service functions as the investigating body of the DPA, with a wide array of investigative powers (e.g., interrogation of individuals).

The front-line service has a singular role in providing guidance (e.g., with regard to adequate data protection techniques under the GDPR) and supervising data controllers and processors and their compliance with data protection legislation.

Led by six experts in the field, the knowledge centre provides public decision-makers with the necessary expertise to understand the technologies likely to impact on the processing of personal data.

The dispute chamber, composed of a president and six judges, is able to impose sanctions of up to €20 million or up to 4 per cent of the total worldwide annual turnover of the infringing company.

As well as the above-mentioned bodies being established under the auspices of the reformed DPA, an independent think tank is set up to reflect society as a whole, both participants in the creation of the digital world and those affected by it, and to provide the executive committee with a broad vision and guidance as it negotiates current and future data protection challenges.

Another novelty of the new DPA is that, along with natural persons, legal persons, associations or institutions will also be able to lodge a complaint of an alleged data protection infringement.

In spite of the expansion of the DPA’s powers, the government had initially announced not to increase its budget. However, it has been reported that the government has put aside €1.6 million for the new DPA to be able to perform its new tasks.

While the new DPA with its new bodies had to be fully functional from 25 May 2018, it ran into some difficulties concerning the nomination of its members. Until this is completed, the new DPA will continue to be headed by its former management, but with all new competences and functions.

### Recent enforcement cases

The most important recent enforcement case undertaken by the DPA is the one initiated against Facebook in June 2015 concerning its unlawful processing of data through hidden cookies. The Court of First Instance has rendered its judgment, condemning Facebook (see above). Facebook has filed for appeal.
The European Court of Justice recently concurred in its judgement in Case C-210/16 with Advocate General Bot and in its judgment stated that the promotion and sale of advertising space by Facebook Germany was inextricably linked to the contested data processing, and therefore German law is applicable. In his non-binding opinion, Advocate General Bot had stated in 2017 that Facebook should indeed adhere to the national privacy rules of EU Member States if it collects and processes data from users in those Member States and has a physical establishment (e.g., a sales office) on their territory. Hence, the advocate general opposed Facebook's argument that it should comply only with Ireland's privacy legislation, the country where it has its European headquarters.

In addition to the Facebook case, the most important enforcement cases before the Belgian courts are the Yahoo! and Skype cases, discussed in Sections II and VI.

### iii Private litigation

Private plaintiffs may seek judicial redress before the civil courts on the basis of the general legal provisions related to tort or, in some cases, contractual liability. In addition, they may file a criminal complaint against the party that committed the privacy breach. Financial compensation is possible, to the extent that the plaintiff is able to prove the existence of damages as well as the causal link between the damage and the privacy breach. Under Belgian law, there is no system of punitive damages.

Class actions were traditionally not possible under Belgian law until 1 September 2014, when a new Act on Class Actions entered into force.

In a judgment of 29 April 2016, the Supreme Court ruled in favour of the right to be forgotten. The case concerned the online disclosure of an archived database of a famous Belgian newspaper, which would result in the publication of the full name of a driver who was involved in a car accident in 1994 in which two people died. Both the Court of Appeal and the Supreme Court considered the right to be forgotten essential in this case and ruled in favour of a limitation of the right of freedom of expression.

### VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

Organisations based or operating outside Belgium may be subject to the Belgian data protection regime to the extent that they process personal data in Belgium. Physical presence in Belgium (either through a local legal entity or branch office, with or without employees, or through the use of servers or other infrastructure located on Belgian territory) will trigger the jurisdiction of Belgian privacy and data protection law even if the personal data that is processed in Belgium relates to foreign individuals. Foreign companies using cloud computing services for the processing of their personal client or employee data may, therefore, be subject to Belgian law (with respect to such processing) if the data is stored on Belgian servers.

In principle, the mere provision of online services to persons in Belgium, without actual physical presence, will not trigger Belgian jurisdiction. However, as discussed under Section VI, according to a recent Supreme Court decision, the Belgian judicial authorities...
would have jurisdiction over foreign entities providing online services or software to users in Belgium, even if they are not present in Belgium. This is certainly an issue to follow up, as it may have an important impact on the territorial scope of application of Belgian law.

It should be noted that the GDPR applies to data controllers having no presence at all (establishment, assets, legal representative, etc.) in the EU but who process EU citizens’ personal data in connection with goods or services offered to those EU citizens; or who monitor the behaviour of individuals within the EU.

IX CYBERSECURITY AND DATA BREACHES

As a member of the Council of Europe, Belgium entered into the Council’s Convention on Cybercrime of 23 November 2001. Belgium implemented the Convention’s requirements through an amendment of the Act of 28 November 2000 on cybercrime, which introduced cybercrime into the Belgian Criminal Code. With the Act of 15 May 2006, Belgium also implemented the requirements of the Additional Protocol to the Convention on Cybercrime of 28 January 2003 concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems.

As previously mentioned, the CCB performs the following tasks:

a. monitoring Belgium’s cybersecurity;

b. managing cybersecurity incidents;

c. overseeing various cybersecurity projects;

d. formulating legislative proposals relating to cybersecurity; and

e. issuing of standards and guidelines for securing public sector IT systems.

Since becoming operational at the end of 2015, the CCB has carried out several awareness campaigns; for instance, in the context of the Petya ransomware cyberattacks and the ‘CEO fraud’ (a large-scale scam where cybercriminals contact a company as the alleged CEO of another big company with a request to make an important payment into the first company’s bank account).

Furthermore, the management of CERT, which has been in the hands of Belnet since 2009, was transferred to the CCB in December 2016. The transfer of all CERT activities is part of the continuing coordination of Belgian cybersecurity and is aimed at assisting companies and organisations in the event of cyber incidents by providing advice both about finding solutions when such incidents arise and about preventing incidents occurring.

Additionally, the Belgian Cyber Security Coalition, which is a partnership between parties from the academic world, public authorities and the private sector, was established in October 2014. Currently, more than 50 key participants from across the three sectors are active members. These include large financial institutions, universities, consultancy companies, professional organisations and government bodies. The main goals of the Coalition are to raise awareness about cybersecurity, exchange know-how, take collective actions in the fight against cybercrime and support governmental and sectoral bodies in setting policies and determining ways to implement these policies.

With respect to data breach notifications, Article 114/1, Section 2 of the Electronic Communications Act requires companies in the telecommunications sector to notify immediately (within 24 hours) personal data breaches to the DPA, which must transmit a copy of the notification to the Belgian Institute for Postal Services and Telecommunications. If there is a breach of personal data or the privacy of individuals, the company must also
notify the data subjects affected by the breach. It is expected that the Belgian implementation of the NIS-Directive will provide for a detailed procedure regarding breaches for operators of essential services (see above).

The Belgian Data Protection Act of 8 December 1992 did not, however, provide for a general data breach notification obligation, as is provided for in the GDPR. In 2013, the DPA was confronted by a series of data security incidents of which it only became aware after those incidents were published in the media. Unable to change the legislation itself (which, of course, would require legislative intervention), the DPA issued a recommendation upon its own initiative stating that it considered data breach notifications to be an inherent part of the general security obligations incumbent on any data controller.

With the entry into force of the GDPR, Article 33 of the GDPR now provides for a duty for the data controller to report personal data breaches to the DPA without undue delay, and where feasible, not later than 72 hours after having become aware of it. This notification must describe the nature, communicate the details of the DPO or other contacts where more information can be obtained, describe the likely consequences of the breach and describe the measures taken or proposed to be taken by the controller to address the breach. A communication can in some cases also be necessary to the data subject, if there is a high risk to their the rights and freedoms. It must be noted that the DPA’s recommendation also stresses that, in the event of public incidents, the DPA must be informed within 48 hours of the causes and damage. Although the concept of a ‘public incident’ is not explained in greater detail, this could refer to an incident in which a breach has occurred that is likely to become known to the public or the DPA via, for example, the media, the internet, or complaints from individuals.

In relation to data security, the International Chamber of Commerce in Belgium and the Federation of Enterprises in Belgium, together with the B-CCentre, have taken the initiative to create the Belgian Cyber Security Guide in cooperation with Ernst & Young and Microsoft. The Guide is aimed at helping companies protect themselves against cybercriminality and data breaches. To that effect, it has listed 10 key security principles and 10 ‘must do’ actions, including user education, protecting and restricting access to information, keeping IT systems up to date, using safe passwords, enforcing safe-surfing rules, applying a layered approach to viruses and other malware, and making and checking backup copies of business data and information.

X OUTLOOK

With regard to the entry into force of the GDPR this year, the overall focus of the DPA will obviously be on assisting companies, data controllers and data processors with the implementation of this new EU data protection framework. To this end, the DPA had launched a new separate section dedicated to the GDPR on its website and a 13-step plan for companies involved in data collection or processing, or both, to help them comply with the forthcoming new rules of the GDPR. That said, months after the entry into force of the GDPR, its website, containing many specific guidelines regarding data protection compliance, still has not been fully updated to reflect the changes made by the GDPR.

Apart from the strengthening of the investigative and sanctioning powers of the DPA (see Section VII), we do not expect the GDPR to result in any major changes to the Belgian
Belgium

situation in practice. Belgium’s legislation and the interpretation given to it by the DPA have traditionally been in line with EU law and the positions of the European Commission and the Article 29 Working Party (now the European Data Protection Board).

As mentioned above (see Section VII), the investigative and sanctioning powers of the DPA will be significantly expanded under the GDPR. In the event of a complaint being lodged with the DPA or of a data breach incident, it will have broader competence to examine the complaint and to impose higher sanctions on the alleged violator. In its assessment of alleged data protection violations, the DPA will definitely check whether sufficient efforts have been made to meet the requirements laid down in the GDPR. Therefore, actual enforcement of data protection legislation may now become more frequent, although it remains to be seen which resources the DPA will have available to actually enforce compliance with the GDPR.

Other than the GDPR, upcoming legislation includes the implementation of the NIS-Directive, meaning that Belgium may obtain a more structured landscape as regards cybersecurity and continuity of essential services. Upcoming European legislation also includes the e-Privacy legislation, which will override the GDPR and provide for more clarity regarding specific issues that may arise concerning privacy in connection with online interactions.
Chapter 7

BRAZIL

Fabio Ferreira Kujawski and Alan Campos Elias Thomaz

I OVERVIEW

The Brazilian Federal Constitution guarantees privacy protection as a fundamental right of all individuals. The Brazilian Civil Code, the Consumer Protection Code, the Information Access Act, the Banking Secrecy Act, the Wiretap Act and the Internet Act are the main statutes governing the processing of personal data, although such statutes apply in specific circumstances, such as in a consumer relationship, in case of data collected online, in case of data controlled by the government, etc.

After years of legislative process, the Brazilian Congress finally approved and the President enacted Law 13,709, of 14 August 2018, the Brazilian Data Protection Law (LGPD). The LGPD was significantly inspired by the General Data Protection Regulation (GDPR) of the European Union. The LGPD establishes detailed rules for the collection, use, processing and storage of personal data in Brazil. This statute is applicable to private and public entities in all economic sectors, both in the digital and physical environment. The LGPD will become effective on 16 February 2020. While the final text of the LGPD approved by Congress provided for the creation of the National Data Protection Authority (DPA), the President vetoed the creation of such entity owing to a flaw in the legislative process. Under Brazil Federal Constitution, the creation of independent regulatory agencies and public functions can only be made by means of a bill submitted to Congress by the President. In the original bill on data protection submitted by the President through the Ministry of Justice, the DPA was not actually created. If the creation of the DPA had not been vetoed by the President, an important constitutional debate would have taken place and the authority of the DPA would have been disputed. It is expected that the President will send another draft bill to the Congress in order to correct the flaw, and allow for the DPA to be properly established as it comes into effect.

Until then, the Public Prosecutor’s Office, the Ministry of Justice, consumer protection authorities (such as the Consumer Protection and Defence Authority (PROCON)) and sector-specific regulatory agencies (such as the Brazilian Central Bank, the Brazilian Securities and Exchange Commission, among others) are handling matters of potential violations of privacy rights in Brazil. Among such authorities, the Federal Prosecutors of the Federal District created a data privacy division, which has turned out to be the most proactive body in prosecuting companies in connection with potential data privacy violations.

1 Fabio Ferreira Kujawski is a partner and Alan Campos Elias Thomaz is an associate at Mattos Filho, Veiga Filho, Marrey Jr e Quiroga Advogados.
II  THE YEAR IN REVIEW

The entry into force of the GDPR in May 2018 and the Cambridge Analytica scandal have prompted the Brazilian Congress to expedite the last stage of debates of the LGPD. Another fact that contributed to the approval of the new legislation was the country’s desire to become a member of the Organisation for Economic Co-operation and Development (OECD), which requires the approval of an omnibus legislation.

As a result, after more than eight years in debate, the LGPD was finally approved; and the impact of this new law is very relevant, not only for Brazilian companies that process personal data in Brazil, but also for any foreign company that processes personal data in the context of offering goods and services to individuals located in Brazil. Just like the GDPR, the LGPD has significant extraterritorial reach.

Aside from the legislation, another important debate took place in the country’s Superior Court of Justice, which considered null and void a consent for intercompany data sharing included in a privacy statement of a large financial institution. The Court took the position that, despite the clear language in the privacy statement accepted by the data subject authorising the sharing of information, the data subject could not freely object to the data sharing and still retain the credit card services it was looking for. As the sharing of information was being made for commercial purposes, so it was not needed to provide the service, the Court deemed the consent invalid on this specific matter.

Another interesting debate is taking place in the Supreme Court, which is analysing the legality of encryption technology that prevents the disclosure of communications content to law enforcement. A decision on this matter is still pending.

III  REGULATORY FRAMEWORK

1 Privacy and data protection legislation and standards

The Federal Constitution and Civil Code

The Federal Constitution rules that intimacy, private life, honour, and image are fundamental rights of all individuals and are inviolable. Individuals who suffer material or moral damage as a result of violation of such rights have the right to indemnification. The Federal Constitution also establishes that one’s mail, data and telephone communications are inviolable, except by authority of a court order and within the context of criminal investigations. The Brazilian Civil Code acknowledges and reinforces the principle that privacy is inherent to an individual’s personality and dignity.

The Brazilian Data Protection Law

The recently approved LGPD establishes detailed rules for the collection, use, processing and storage of personal data in Brazil. This omnibus law is applicable to any processing activity of personal data carried out by a natural person or legal entity, regardless of the means of

2 The LGPD is not applicable to processing activities (1) performed by natural persons, exclusively for private and non-economic purposes; (2) for journalistic, artistic and academic purposes; (3) for public and state security, and national defence purposes; (4) for investigation and prosecution of criminal offences; and (5) for data transiting through Brazil, without any processing in the country.
processing (i.e., digital or not) and where the processor is headquartered, provided that the processing is carried out in Brazil; the processing relates to the offer or supply of goods or services in Brazil; or the data was collected in Brazil.

Under the LGPD, personal data is defined as ‘information related to an identified or identifiable natural person’. Any processing activity shall be made in accordance with the principles set forth therein³ and based on one or more of following legal bases for data processing provided for in such law:

- consent;
- compliance with a legal or regulatory obligation;
- when necessary for the performance of a contract or preliminary procedures related to contract of which the data subject is a party, at the request of the data subject;
- when necessary to meet the legitimate interest of the data controller or third parties;
- protection of the life or physical safety of the data subject or third party;
- protection of health, in proceedings carried out by health professionals or by health entities;
- by research bodies, to carry out studies, guaranteed, whenever possible, the anonymisation of personal data;
- by the public administration, for the execution of public policies; and
- protection of credit.

The LGDP draws a distinction between personal data and sensitive data and imposes a higher bar for allowing processing of this kind of data.⁴ Sensitive data shall mean any information related to a data subject concerning racial or ethnic origin, religious beliefs, political opinions, membership of trade unions or religious, philosophical or political organisations, health, sexual life, genetics or biometrics.

When relying on consent, the LGPD imposes specific requirements. So, the consent shall be prior, free, informed and unequivocal. For sensitive data, in addition to such requirements, the consent must be specific and given separately from other consents.

---

³ The principles of the LGPD are as follows: free access (free and easy consultation of data processing activities and their duration); transparency (clear, accurate and easily accessible information); purpose (processing must be carried out for legitimate, specific, explicit and stated purposes, and no further processing shall take place when incompatible with such purposes); adequacy (processing shall be compatible with the stated purpose); data quality (assurance that the data is accurate, clear, relevant and up to date); data minimisation or necessity (processing shall be limited to the minimum information necessary to achieve its purpose, using relevant, proportional and not excessive data); security (use of technical and administrative measures capable of protecting personal data from unauthorised access and from accidental or unlawful events of destruction, loss, alteration, communication or dissemination); prevention (adoption of measures to prevent the occurrence of damages); non-discrimination (processing should not be unlawful or discriminatory); accountability (demonstration of effective measures for complying with the rules);

⁴ The lawful bases for processing sensitive data include: (1) consent; (2) compliance with a legal or regulatory obligation; (3) regular exercise of rights, including in contract and in judicial, administrative and arbitral proceedings; (4) protection of life or physical safety of the data subject or third party; (5) protection of health, in proceedings carried out by health professionals or by health entities; (6) when necessary to guarantee the prevention of fraud and safety of the data subject, in the process of identification and authentication in registries of electronic systems; (7) by the public administration, for shared processing of data necessary for the performance of public policies set forth in law or regulation; and (8) by research bodies, to carry out studies, guaranteed, wherever possible, the anonymisation of data.
Several other rights have been granted to data subjects, such as the right to obtain information regarding the processing of data, right to access, to rectify and erase data, right to withdraw the consent, to receive information to whom the data has been shared, the right to data portability and the right to obtain the review of automated decisions.

The new law also provides for limitations to international data transfers as further detailed below. The LGPD also contemplates data incident reporting obligations (see Section IX below).

Anonymised data is out of the realm of the LGPD. Anonymised data was defined as a data of an individual who cannot be identified, using reasonable technical means available at the time the processing takes place.

Other statutes dealing with the processing of personal data, such as the Consumer Protection Code, the Wiretap Act, the Banking Secrecy Act, the Information Access Act and the Internet Act shall continue to apply, to the extent that they do not conflict with the LGPD.

ii  Penalties for non-compliance

Violation of privacy rights gives rise to compensation for moral and direct damage. Non-compliance with the provisions of the LGPD may result in warning, mandatory disclosure of the data incident, deletion of personal data, temporary blocking and fines of up to 2 per cent of the infringing company’s economic group net turnover in Brazil in the preceding fiscal year, limited to 50 million reais per violation.

iii  General obligations for data handlers

The LGPD defines two categories of data handlers, the ‘controllers’ and ‘operators’ (jointly referred as ‘processing agents’). Inspired in the definition of controllers and processors under the GDPR,5 the LGPD defines controllers as ‘natural person or legal entity, public or private, which is responsible for the decisions concerning the processing of personal data’, and operators as ‘natural person or legal entity, public or private, which performs the processing of personal data on behalf of the controller’.

Processing agents, in any case, shall abide by the data processing principles set forth in the LGPD and adopt technical and organisational measures to protect personal data from data incidents.6

According to the LGPD, data controllers must: (1) define and document the legal basis for processing personal data (record of processing); (2) guarantee the implementation of mechanisms to comply with data subjects’ rights; (3) report data breaches and security

5 In the GDPR, ‘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; and ‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

6 Data incident may be considered as ‘unauthorised access and from accidental or unlawful destructions, loss, change, communications, transmission, or any other occurrence resulting from inadequate or illegal processing’.
incidents to the DPA and, in some cases, to the affected data subjects; (4) perform privacy impact assessments (where required by the DPA); and (5) appoint a data protection officer, who will be in charge of handling personal data within the organisation.

In addition, data controllers shall make easily accessible to the data subject a fairly detailed privacy notice, stating clear, adequate and ostensive information on the purposes of the data processing; form and duration of the data processing; contact information of the controller; information regarding the shared use of personal data by the controller; responsibilities of the processing agents; and data subjects’ rights.

If the privacy notice is drafted in such a way as to significantly reduce the privacy rights recognised by law, there is a chance that it shall be deemed invalid. Even before the LGPD, Brazilian courts have been systematically striking down privacy notice provisions that imply a waiver of all or substantially all of an individual’s privacy rights.

There is no requirement for registration of databases in Brazil.

The LGPD also defines the mandatory reporting of data incidents, as further detailed below.

iv Specific regulatory areas

Consumer Code

The Consumer Code establishes certain data protection rights to be observed in a consumer relationship, including the deletion of negative creditworthiness information exceeding five years; and rectification of data within the period of five days.

Internet Act

Under the Internet Act, internet connection providers (i.e., those that offer telecommunications connectivity for internet access) cannot monitor or store any information concerning the use of the internet by their users. Internet connection providers are required to retain connection logs for a minimum period of 12 months. Connection logs must include the date, time and duration of an internet connection made by a certain IP address provided by the connection provider to the user.

Internet application providers (i.e., those that offer any kind of functionality to their users through the internet, such as social networks, e-commerce websites, etc.) shall store access logs for at least six months. In such cases, access logs must include the date, time and duration of connections to the internet application made by a certain IP address.

Under the Internet Act, express consent is always required for collecting data online. Upon the creation of the LGPD, we are of the opinion that the other lawful basis provided for in the new statute shall also apply to data collected online. Furthermore, the consent attributes shall be those approved by the LGPD and no longer those of the Internet Act. In other words, no express consent shall be required for data collected online when the LGPD becomes effective.

Information handled by public authorities

The Information Access Act governs the collection, use and processing of data by the federal government. This law also establishes rules and procedures by which citizens can request details of the information processed by public authorities.
**Banking Secrecy Act**

Financial institutions, such as banks, credit card administrators and the stock exchange must maintain strict confidentiality of financial transactions and financial information of their clients, pursuant to Complementary Law No. 105/01. The exchange of data between financial institutions for credit profiling and risk management is allowed in specific circumstances. Financial institutions shall report to relevant authorities any transaction they deem suspicious (under anti-money-laundering regulations), and such reporting shall not be considered a breach of confidentiality duties. Specific and detailed cybersecurity requirements are imposed on financial institutions, including specific limitations to contract data processing and cloud services (Central Bank Resolution 4,658/2018), the same applying to payment companies.

**Health**

The Medical Ethical Conduct Code (Federal Council of Medicine, Resolution 1,931/2009) provides for certain rules on the protection of patients’ information and medical records. A specific resolution issued by the Federal Council of Medicine governs the use of computer systems for storage, handling and retention of such data, authorising the replacement of paper with electronically stored information. In any case, with the enactment of the LGPD, the processing of sensitive data (which includes medical information) shall only occur on the basis expressly allowed by the LGPD.

**Telephone or radio communications**

The confidentiality of telephone and computer communications is protected by the Wiretap Act (Law 9,296/96) and the Telecommunications Act (Law No. 9,472/97). The access to and interception of telephone and telematics communications may only occur under the authority of a valid court order in criminal investigation proceedings. Pursuant to the Telecommunications Act, the use of clients’ information can only be made for the purpose of delivering telecommunication services.

**Employees**

Employees are subject to data protection rights under the LGPD. The employers are allowed to process employees’ data for the purposes of managing the employment relationship. The legal basis for processing may be compliance with legal obligation, performance of a labour contract or legitimate interest of the controller. Therefore, consent is not required for processing data relating to the management of labour relationship, even in case of sensitive data. Employee data may be used by the employer and transferred to other affiliate entities for the purpose of managing the employment relationship (for use by a centralised back office, HR-related activities, etc.), provided that the requirements of international transfer are observed.

Employers are allowed to monitor the use of equipment and IT systems offered by the employer, so employees should not expect privacy on such environments. The majority of legal scholars and most of the decisions rendered by the court of appeals sustain this position. All equipment and devices provided by the employer to their employees for the exercise of the employees’ functions within the company shall be deemed company property and therefore may be subject to surveillance. For companies that install their systems into employee’s devices (BYOD), we also believe that surveillance on such devices is possible to the extent that it focuses only on the employer’s information. Finally, Brazilian laws do not
restrict the use of surveillance video systems, provided that the recording or videotaping is not performed in areas where any kind of embarrassment is inflicted on the employee (e.g., cameras installed in bathrooms).

**Electronic marketing**

Marketing campaigns by email are likely to be deemed legitimate under the opt-in or ‘soft opt-in’ system, but shall always allow the data subject to opt-out from receiving such messages. The telecommunications regulators determined that mobile carriers are only allowed to send promotional messages to their users who have expressly accepted receiving them.

**Child protection**

The Child and Adolescent Act (Law No. 8,069/1990) stipulates that the offer, exchange, delivery, transmission, distribution, publication or disclosure of photographs, videos or other materials containing explicit sex scenes or child pornography is a criminal activity, which will be subject to a penalty of up to eight years of imprisonment. The LGPD adds additional protection to child’s personal data. Among other provisions, it determines that information should be provided in a simple, clear and accessible manner to the child and the processing agent shall use reasonable efforts to verify that the consent was given by the child’s legal representative.

**Exercise of profession**

Other federal statutes cover legal profession privilege, such as attorney–client privilege.

**Technological innovation**

Brazil has a new data protection legislation, which may significantly increase data subjects’ rights and control over their data. While the protection of personal data is certainly positive in many instances, the law should not be interpreted in a way to materially impact the development of new technologies that may bring important benefits to the country.

As such, the use of anonymised data should be encouraged and right of privacy shall be read in conjunction with other principles and values embraced by other laws and the Federal Constitution.

Section 2 of the LGPD states that innovation, economic and technologic development and free enterprise constitute cornerstones of the new law. As a result, significant importance shall be given to the controller’s legitimate interest in processing data, as well as processing to meet public interest objectives (such as health, education, agriculture, smart cities and urban mobility, among so many others). Many upcoming technologies in the space of IOT and artificial intelligence are boosting innovation and being instrumental for this technological revolution. Government and enforcement authorities should be aware that their actions may significantly impact the pace by which the country may benefit from all such developments.

The key is to balance privacy rights with all other rights afforded to individuals and legal entities. No right should be interpreted on a stand-alone basis.

**IV INTERNATIONAL DATA TRANSFER AND DATA LOCALISATION**

The LGPD imposes certain requirements for international data transfer, which can only take place in the following circumstances:
a to countries with an adequate level of protection (to be determined by the DPA);
b through the use of standard contractual clauses, binding corporate rules, seals, certificates and codes of conduct approved by the DPA;
c upon specific consent of the data subject, with prior information on the international character of the operation;
d to comply with a legal or regulatory obligation;
e when necessary for the performance of a contract;
f for the protection of life and physical safety of the data subject or third party;
g for the regular exercise of rights in judicial, administrative or arbitral proceedings;
h when necessary for international legal cooperation between intelligence, investigation and prosecutors;
i when authorised by the DPA; and
j when necessary for the execution of public policy or compliance with the legal attribution of the public service.

Until the LGPD becomes effective, there is no specific regime or regulation regarding the transfer of data outside Brazil. As a rule, if the notice or consent was provided (when required) and the relevant privacy policy expressly provides for the international data transfers, international transfer was allowed.

Except for sector-specific regulations (e.g., applicable to the processing of government and financial data), Brazilian laws do not impose data localisation requirements.

V COMPANY POLICIES AND PRACTICES

With the enactment of the LGPD, private and public organisations will have to adjust their privacy policies and practices to become compliant with the new legal standards.

There are two different dimensions to this matter. One dimension is the customer-facing policies that will have to be adapted to conform with the LGPD. Companies will have to determine whether their right to process data is compatible with the new law. This means investigating all lawful bases for data processing. Even when the processing is made on the basis of consent, one must ensure that the consent meets the requirements of being free, previous, informed and unequivocal. Where consent is not available, one may determine if there is any other legal basis for processing data, such as the obligation to perform a contract, compliance with law or even the controller’s legitimate interest.

The data controller must record all decisions concerning the processing of data, and these records may be required by the DPA.

Conducting privacy impact assessment is also advisable when any processing operation may pose a significant risk to the data subject, and notably when the basis for processing is the controller’s legitimate interest. Privacy by design is also part of the LGPD, so companies should be used to create new products, services or technologies applying the right principles of data treatment (such as data minimisation, transparency, right of access and deletion of data, portability, etc.).

As far as data incidents are concerned, the companies shall permanently train their personnel on the company’s policies concerning data processing, confidential information, intellectual property rights, trade secrets, among other related matters.
VI DISCOVERY AND DISCLOSURE

An internet application provider shall only be compelled to disclose user access logs and information under the authority of a valid court order. Interception of telephone and internet communication may only occur in limited circumstances and by authority of a valid court order in the context of criminal investigation proceedings.

Brazilian judges have systematically argued that Brazilian court orders should be complied with by Brazilian subsidiaries of the data controllers who actually processes data outside Brazil. Frequently, the order is directed to local subsidiaries of internet service providers (ISPs) that do not host the required information locally. These subsidiaries used to claim lack of procedural standing (as the information is held by the parent company) or that a formal recognition process (e.g., MLAT) should be adopted to allow such order to produce effects out of Brazil. Although these arguments have been raised by several internet companies, they have been repeatedly rejected by Brazilian courts.

Therefore, the current trend is to impose the obligation on the entity that may have access to the requested information (and, therefore, has the means to deliver the information), rather than on the entity considered to be the original data handler. The place where the information is actually hosted has largely tended to become irrelevant as cloud computing solutions are increasingly adopted.

With the increased use of voice over internet protocol and messaging services protected by strong encryption, complying with interception or content disclosure orders have become more challenging. The increased number of requests for disclosure of metadata, on the other hand, has shown that other types of information may also be relevant for criminal prosecution purposes.

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

Until the creation of the DPA, no specific regulatory agency or public administrative body was specifically designated to regulate and enforce data privacy laws. Typically, investigations are initiated by the Public Prosecutor’s Office, consumer protection authorities (such as PROCON) and other consumer protection associations. Administrative proceedings may be either civil or criminal, and may lead to the filing of civil or criminal public lawsuits, as the case may be. The administrative and judicial proceedings are subject to due process, so the defendant may put together an adequate defence and produce all evidence deemed important. Under the Consumer Laws, penalties are generally applied up to 10 million reais. Moral damages may also be imposed and Brazilian courts generally award up to 1 million reais for these types of damages. The payment of such damages may be on the top of individual claims. Under the Internet Act, violations of privacy rights may give rise to indemnification of up to 10 per cent of the infringing entity’s net turnover in Brazil in the previous fiscal year. Under the LDPG, penalties may be imposed of up to 2 per cent of the Brazilian turnover of the infringing entity’s economic group in the previous fiscal year. We are of the opinion that

---

7 One exception to this rule relates to the rights of police authorities and prosecutors to request limited information (such as name, ID number, address and parents’ name of an individual) without a court order.
the same violation should not give rise to a double penalty. Therefore, if there is a violation of privacy rights, the penalties of the Internet Act or the penalties under the LGPD should apply but not both.

ii Recent enforcement cases

There are many administrative proceedings initiated against entities in Brazil, either with respect to data breaches or to alleged illegal processing. We already mentioned a decision issued by the Superior Court of Justice deeming invalid a consent for intercompany data sharing made by a major financial institution. Other high-profile cases not yet settled involved a major urban mobility app, one of the major sporting apparel e-commerce portals, and a major provider of software company that was prevented from collecting data from the internet browser embedded by OEMs into computers. In another interesting case, the Department of Consumer Protection and Defence imposed a fine of 7.5 million reais for adopting geopricing techniques, by which consumers would pay different prices for equal services depending on the user's location.

iii Private litigation

Because Brazil is among the countries with the highest number of internet users, private litigation has been significantly increasing in recent years, fostered by technological developments and proliferation of websites and service providers, many of which are unaware of laws and regulations in Brazil. The most common private claims involve: indemnification for breach of privacy or provision of defective products or service (including lack of safety or proper warnings); user and content takedown; and supply of data by the offender (connection and access logs, which are used to identify individuals who may have committed offences through the internet).

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

Even before the enactment of the LGPD, Brazilian courts were accepting the processing of cases under Brazilian law and local jurisdiction despite the relevant service agreements or terms of use establishing foreign law and jurisdiction. Virtually no Brazilian court decisions recognised the choice of foreign law and jurisdiction in consumer agreements.

The Internet Act and the LGPD establishes that Brazilian law shall apply to any processing activity performed in Brazil, related to individuals located in Brazil or collected from an user located in the country. Brazilian law shall apply even if the service provider is domiciled abroad.

When the data controller is located abroad but holds a subsidiary in Brazil, this subsidiary will be recognised as holding procedural standing in any claim (either initiated by an individual or by the consumer protection authorities). In the past, local subsidiaries used to argue that they would lack standing, as the servers are not in Brazil and they could not have access to it. The Brazilian judiciary has systematically denied this position, so raising this jurisdictional argument is ineffective and does not contribute to creating a positive reputation for a company.
IX CYBERSECURITY AND DATA BREACHES

Organisations processing personal data shall observe the cybersecurity requirements imposed by the LGPD. Data controllers and processors shall adopt technical and organisational measures to protect personal data from unauthorised access and from accidental or unlawful destructions, loss, change, communications, transmission, or any other occurrence resulting from inadequate or illegal data processing (a data incident). Except in limited circumstances, data incidents may trigger liabilities. The Consumer Code also provides that companies shall take all reasonable measures to offer safe and free-of-defect products and services. Therefore, if the organisation does not implement appropriate security measures (normally based on industry standards or best practices) a product or service may be deemed defective and trigger liabilities.

In addition, the LGPD requires data controllers and processor to adopt data protection measures since the creation of any new technology or product, which will require organisations to adopt a privacy by design approach.

Data incidents that may result in relevant risk or harm to individuals must be reported to DPA\(^8\) within a reasonable time\(^9\) and, where required by the DPA or otherwise by law, to the affected data subjects.

The DPA does not prevent other cyber-related statutes from being imposed by sectoral agencies, such as the Brazilian Central Bank with Resolution 4,658/2018.

X OUTLOOK

With the approval of the LGPD, organisations will have to adapt their privacy policies, notices and internal processes to become compliant with the new legislation. Multinational organisations are likely to be subject to more than one regulatory regime on the matter, such as those that process data related to individuals located in Brazil and in the European Union, which will have to comply not only with the LGPD, but also with the GDPR. More awareness and protection of data subjects’ rights and increasing enforcement action from Brazilian authorities are certainly expected in years to come.

---

\(^8\) Specific information needs to be provided, including, at least: (1) a description of the data and individuals affected; (2) the risks related to the data incident; (3) the reasons why the notification to the DPA has been delayed, if applicable; and (4) the technical and security measures taken to protected the data, and the measures that were or will be taken to revert or mitigate the effects of the data incident.

\(^9\) Unlike the GDPR, there is no particular deadline for notification (e.g., 72 hours). In any case, it cannot be unreasonably delayed and the DPA or any further decree may impose a maximum reporting time frame.
Chapter 8

CANADA

Shaun Brown

I OVERVIEW

Privacy in Canada is regulated through a mix of constitutional, statutory and common law. The most fundamental protection is provided by Section 8 of the Charter of Rights and Freedoms, which states that ‘everyone has the right to be secure against unreasonable search or seizure’. This ensures a reasonable expectation of privacy for citizens in relation to the state.

There are also laws that apply to the collection, use and disclosure of personal information by organisations in the public and private sectors at the federal, provincial and territorial levels. Finally, organisations in both sectors are increasingly required to defend privacy-related lawsuits based on statutory and common law torts.

This chapter focuses on the aspects of Canadian privacy law that apply to private sector organisations.

II THE YEAR IN REVIEW

In June 2017, the federal government delayed the private right of action under Canada’s anti-spam legislation (CASL), which was set to come into effect on 1 July. The private right of action would allow any person affected by violations of the law to sue for actual and statutory damages. The government cited concerns raised by businesses, charities, and not-for-profit organisations in its reasons for the delay. At the same time, the government asked the House of Commons Standing Committee on Industry, Science and Technology (INDU) to conduct a statutory review of the legislation.

INDU issued a report following completion of its review in December of 2017, making 13 recommendations that focus on providing organisations with greater clarity on how CASL

---

1 Shaun Brown is a partner at nNovation LLP.
2 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 (SC 2010, c 23), s 47 [CASL].
is intended to apply. The committee also recommended that the government wait to assess the impact of such clarifications before determining whether and how to proceed with the private right of action.

The government published its response to the INDU report in March 2018, agreeing that the Act and its regulations require clarification to reduce the costs of compliance and improve enforcement, without committing to any time frame to address such concerns.

On 27 March 2018, the federal government published final regulations that provide further detail on the pending privacy breach notification requirement under the federal Personal Information Protection and Electronic Documents Act (PIPEDA). As of 1 November 2018, private sector organisations subject to the law will be required to notify affected individuals and report to the Privacy Commissioner of Canada any breach of security safeguards resulting in a real risk of significant harm to individuals.

In February 2018, the Standing Committee on Access to Information, Privacy and Ethics (ETHI) tabled its report following a detailed review of PIPEDA. ETHI made several recommendations for significant changes to the law, which centred around four themes: consent; online reputation; stronger enforcement powers of the Privacy Commissioner of Canada; and, the impact of the European Union's General Data Protection Regulation (GDPR) on PIPEDA's adequacy. If implemented, the committee’s recommendations would align PIPEDA much more closely with GDPR.

The government issued its response to the ETHI report on 19 June 2018. The response generally acknowledged the concerns raised in the report and reiterated that any proposed change would require further study and need to account for the views of all stakeholders. The government did not agree with the review’s recommendation that PIPEDA include a framework for de-indexing and erasure of personal information given the potentially far-reaching impacts of both rights (e.g., their potential impact on freedom of speech and on public records) and its inconsistency with the commercial application of PIPEDA.

The Federal Court of Canada affirmed that PIPEDA applies to organisations that collect, use and disclose personal information about Canadians in the course of commercial activity, even where those organisations have no physical presence in Canada.

© 2018 Law Business Research Ltd
PIPEDA when it found that a debtor who defaulted on a loan had given implied consent to the debtor’s bank to disclose a mortgage statement to the lender so that it could enforce a judgment through the sale of the debtor’s home.¹¹

III REGULATORY FRAMEWORK

i Overview of privacy and data protection legislation and standards

Private sector organisations are subject to privacy legislation that governs the collection, use and disclosure of personal information in the course of commercial activities throughout Canada. Organisations must be cognisant of the various laws that exist at the federal and provincial levels due to shared jurisdiction over the regulation of privacy.

The federal PIPEDA, which began to come into force on 1 January 2001, applies to organisations that are federally regulated, including telecommunications service providers, railways, banks and airlines. It also applies to provincially and territorially regulated organisations in provinces and territories that have not passed their own private sector privacy legislation deemed ‘substantially similar’ to PIPEDA. Only three provinces currently have such substantially similar private sector privacy legislation in force: Alberta, British Columbia and Quebec.¹²

Although there are some differences between these laws, they are generally quite similar in application. Most importantly, these laws are all based on fair information practice principles established under the Canadian Standards Association Model Code for the Protection of Personal Information¹³ (CSA Model Code), which is incorporated directly into the text of PIPEDA. The CSA Model Code, which was developed through a collaborative effort involving industry, government and consumer groups and adopted in 1996, establishes the following 10 principles:

a accountability;
b identifying purposes;
c consent;
d limiting collection;
e limiting use, disclosure and retention;
f accuracy;
g safeguards;
h openness;
i individual access; and
j challenging compliance.

¹² Alberta: Personal Information Protection Act, SA 2003, c P-6.5; British Columbia: Personal Information Protection Act, SBC 2003, c 63; Quebec: An Act respecting the Protection of Personal Information in the Private Sector, RSQ, c P-39.1. PIPEDA also does not apply to the collection, use and disclosure of personal health information by personal health information custodians that are subject to the New Brunswick Personal Health Information Privacy and Access Act, SNB 2009, c P-7.05, the Newfoundland and Labrador Personal Health Information Act, SNL 2008, c P-7.01 or the Ontario Personal Health Information Protection Act, 2004, SO 2004, c 3, Sch A. Manitoba has passed private sector privacy legislation – the Personal Information Protection and Identity Theft Prevention Act, CCSM c P33.7) – that is generally similar to the laws in Alberta and British Columbia; however, it has neither been proclaimed in force nor deemed substantially similar to PIPEDA.
Definition of personal information

The most important concept in privacy legislation is ‘personal information’. Personal information is defined broadly as ‘any information about an identifiable individual’. The Supreme Court of Canada has held that this definition must be given a broad and expansive interpretation.\(^{14}\)

Personal information includes such things as a person’s name, race, ethnic origin, religion, marital status, educational level, email addresses and messages, internet protocol (IP) address, age, height, weight, medical records, blood type, DNA code, fingerprints, voiceprint, income, purchases, spending habits, banking information, credit or debit card data, loan or credit reports, tax returns, social insurance number or other identification numbers.

Information does not need to be recorded for it to be personal. For example, information could be in the form of an oral conversation, or real-time video that is not recorded.\(^{15}\)

Information must be about a person who is ‘identifiable’ to be ‘personal’. The Federal Court of Canada has held that: ‘information will be about an identifiable individual where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other available information’.\(^{16}\)

The Privacy Commissioner of Canada (Commissioner), who is responsible for oversight of PIPEDA, has taken an expansive approach to this question in the past. For example, in one investigation involving the use of deep packet inspection technologies by an internet service provider (ISP), the Commissioner held that the IP addresses collected by the ISP were personal information even though they were not linked to individuals, because the ISP had the ability to make such a link.\(^{17}\)

Perhaps even more notable is the Commissioner’s approach to online behavioural advertising (OBA). The Commissioner has taken the position that much of the information used to track and target individuals with interest-based advertisements online – including such things as IP addresses, browser settings, internet behaviour – is personal information even where individuals are not personally identified. The Commissioner explained that:

\[\text{In the context of OBA, given the fact that the purpose behind collecting information is to create profiles of individuals that in turn permit the serving of targeted ads; given the powerful means available for gathering and analyzing disparate bits of data and the serious possibility of identifying affected individuals; and given the potentially highly personalised nature of the resulting advertising, it is reasonable to take the view that the information at issue in behavioural advertising not only implicates privacy but also should generally be considered ‘identifiable’ in the circumstances. While such an evaluation will need to be undertaken on a case-by-case basis, it is not unreasonable to generally consider this information to be ‘personal information’.}\]

\(^{14}\) Dagg v. Canada (Minister of Finance) [1997] 2 SCR, dissenting, 403 at Paragraph 68.


\(^{16}\) Canada (Information Commissioner) v. Canada (Transportation Accident Investigation and Safety Board), 2006 FCA 157, Paragraph 34.


There are few precedents in Canadian law that have restrained this expansive approach to interpreting personal information.

To varying degrees, privacy laws contain exceptions for business contact information, including the name, title and contact information for a person in a business context. As of June 2015, ‘business contact information’, including the ‘position name or title, work address, work telephone number, work fax number or work electronic address’ of an individual was excluded from PIPEDA.

iii  General obligations for data handlers

As described above, privacy legislation is based on 10 fair information practice principles. This section provides a brief description of the primary obligations for data handlers arising under each of these principles.

Principle 1 – accountability

‘An organisation is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organisation’s compliance with the following principles.’

Accountability speaks to the obligations of organisations to establish privacy-related policies and procedures, and to designate staff who are responsible for ensuring that an organisation is compliant with privacy legislation. Organisations are also expected to provide employees with privacy training.

The accountability principle imposes obligations on organisations to ensure that personal information is adequately protected when transferred to a third party for processing. Accordingly, organisations that rely on service providers to process personal information on their behalf (e.g., payroll services) must, through contractual means, ensure that personal information will be handled and protected in accordance with privacy legislation. This requirement applies regardless of whether personal information is transferred to an organisation within or outside Canada.

Principle 2 – identifying purposes

‘The purposes for which personal information is collected shall be identified by the organisation at or before the time the information is collected.’

Often referred to as providing ‘notice’, organisations are required to document and identify the purposes for collecting personal information. This principle is closely related to the requirement to obtain consent as well as the openness principle.

Notice must be properly targeted to the intended audience. This can pose a challenge as the Commissioner expects organisations to fully explain sometimes complicated technical issues (e.g., OBA) in a manner that can be easily understood by any person who may use the organisation’s product or service. It is for this reason that the Commissioner often recommends the use of ‘layered’ privacy notices to explain more technical issues.

Principle 3 – consent

‘The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except when inappropriate.’

Of the 10 principles, consent is possibly the single most important and complex requirement. As a general rule, organisations are required to have consent before collecting,
using or disclosing personal information. For consent to be valid under PIPEDA, it must be reasonable to expect that the individual would understand the nature, purposes and consequences of the collection, use or disclosure of his or her personal information.

Consent can either be express or implied. Although the concept is somewhat flexible, ‘express consent’ generally means that a person provides some form of affirmative indication of their consent. It is for this reason that express consent is often equated with ‘opt-in’ consent. Alternatively, as stated in the CSA Model Code, ‘implied consent arises where consent may be reasonably inferred based on the action or inaction of the individual’.

Whether consent can be express or implied depends on a few factors. Express consent is almost always required whenever ‘sensitive’ personal information is involved. This includes, for example, information pertaining to a person’s race or ethnicity, health or medical condition, or financial information (e.g., income, payment information).

The concept of ‘primary purpose and secondary purposes’ is also relevant to the form of consent required. A primary purpose is one that is reasonably necessary to provide a product or service; for example, the collection and use of an individual’s address may be necessary to deliver a product ordered online. In this case, consent would be implied to collect and disclose an individual’s mailing address to a delivery company.

However, marketing or advertising is almost always considered a secondary purpose. For example, an organisation would require express consent to collect and disclose an individual’s mailing address to a third party for the purpose of sending marketing materials.19

Note that organisations are prohibited from requiring an individual to consent to the collection, use or disclosure of personal information for a secondary purpose as a condition of providing a product or service.20

A third form of consent, which is sometimes viewed as falling between express and implied consent, is ‘opt-out’ consent. Opt-out consent means that an individual is provided with notice and the opportunity to express non-agreement to a given collection, use or disclosure. Otherwise, consent will be assumed. The Privacy Commissioner has held that it is acceptable to rely on opt-out consent so long as the following conditions are met:

1. the personal information is demonstrably non-sensitive in nature and context;
2. the context in which information is shared is limited and well-defined as to the nature of the personal information to be used or disclosed and the extent of the intended use or disclosure;
3. the organisation’s purposes are limited and well defined, stated in a reasonably clear and understandable manner, and brought to the individual’s attention at the time the personal information is collected;
4. the organisation obtains consent for the use or disclosure at the time of collection, or informs individuals of the proposed use or disclosure, and offers the opportunity to opt out, at the earliest opportunity; and

---

19 An exception to this rule is PIPEDA Case Summary #2009-008 – Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc under the Personal Information Protection and Electronic Documents Act, in which the Assistant Privacy Commissioner of Canada held that because revenues from advertising allow Facebook to offer a free service, the collection, use and disclosure of personal information for advertising is therefore a ‘primary purpose’, and ‘persons who wish to use the service must be willing to receive a certain amount of advertising’. As such, it is acceptable for Facebook to require users to consent to certain forms of adverts as a condition of using the site.

20 This is often referred to as ‘refusal to deal’.
the organisation establishes a convenient procedure for opting out of or withdrawing consent to secondary purposes, with the opt-out taking effect immediately and before any use or disclosure of personal information for the proposed new purposes.21

There are a number of exceptions to the need to obtain consent for the collection, use or disclosure of personal information, including the following:

a for a purpose that is clearly in the interest of the individual and consent cannot be obtained in a timely way (e.g., emergencies);
b for purposes related to law enforcement activities, or to comply with warrants or court orders;
c where personal information is ‘publicly available’ as defined under privacy legislation;22 and
d in business transactions (e.g., sale of a business), provided that the parties agree to only use and disclose personal information for purposes related to the transaction, protect the information with appropriate security safeguards, and return or destroy the information where the transaction does not go through.

**Principle 4 – limiting collection**

‘The collection of personal information shall be limited to that which is necessary for the purposes identified by the organisation. Information shall be collected by fair and lawful means.’

This principle is relatively simple and self-explanatory: organisations must not collect more information than is required for a stated purpose.

**Principle 5 – limiting use, disclosure and retention**

‘Personal information shall 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. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.’

Related to the previous principle, organisations must not use or disclose personal information for purposes beyond those for which the information was originally collected. If an organisation seeks to use or disclose personal information for a new purpose, then consent must be obtained.

Organisations are required to establish clear retention policies and securely destroy information that is no longer necessary. Although it may be tempting for organisations to retain information indefinitely given the low cost of data storage, a failure to establish retention policies risks a violation of this principle. Moreover, not having retention policies can substantially increase an organisation’s risks and costs in the event of a data breach.

---


22 The definition of ‘publicly available’ is relatively limited under Canadian law. For example, according to the Regulations Specifying Publicly Available Information SOR/2001-7 under PIPEDA, personal information is publicly available if it appears in a telephone directory, business directory, a court or judicial document, or a magazine or newspaper. In its response to a 2018 review of PIPEDA (see note 23), the government stated that it needs to closely study the potential impacts of redefining ‘publicly available’ information for the purpose of PIPEDA.
**Principle 6 – accuracy**

‘Personal information shall be as accurate, complete and up to date as is necessary for the purposes for which it is to be used.’

Organisations have an obligation to ensure that personal information is accurate and up to date; however the degree of accuracy may depend on the purpose for which the information is used. For example, there may be a heightened obligation to ensure the accuracy of credit information given that this information forms the basis of significant financial decisions about an individual.\(^{23}\)

Despite this general obligation, organisations are prohibited from routinely updating personal information where it is unnecessary to do so.

**Principle 7 – safeguards**

‘Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.’

Organisations are required to implement physical, administrative and technical measures to prevent the loss, theft, and unauthorised access, disclosure, copying, use or modification of personal information.

Canadian law is not prescriptive with respect to safeguards. Moreover, specific measures can depend on certain factors, such as the sensitivity of information involved, foreseeable risks and harms, and the costs of security safeguards. That said, the Privacy Commissioner expects that organisations implement certain measures – such as: the use of encryption technologies whenever possible, and especially where sensitive personal information is involved; limiting access to personal information to those employees who require access and who are required to sign an oath of confidentiality; and maintaining audit logs of databases containing personal information.

The Alberta Personal Information Protection Act was the first private sector law with an explicit requirement to notify individuals in the case of a security breach.\(^ {24}\) Once in force, recent amendments to PIPEDA will require organisations to notify the Privacy Commissioner and affected individuals of any breach of safeguards if it is reasonable to believe in the circumstances that the breach poses a real risk of significant harm. Failure to comply with the new notification requirements once they are in force could result in a penalty of up to C$100,000.

**Principle 8 – openness**

‘An organisation shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.’

As stated above, the openness principle is closely related to Principle 2 – identifying purposes. Essentially, this Principle requires organisations to provide privacy policies (or notices). Privacy policies are expected to meet the following requirements:

1. provide a full description of what information is collected, used and disclosed, and for what purposes;

---

\(^{23}\) The Federal Court emphasised this obligation in *Nammo v. TransUnion of Canada Inc*, 2010 FC 1284, in which the applicant was denied a loan as a result of information provided by TransUnion that was described as ‘grossly inaccurate’. The Court awarded damages of C$5,000.

\(^{24}\) See Personal Information Protection Act, SA 2003, Sections 34.1 and 37.1.
be easily accessible, accurate and easily understood by the average person;
c inform an individual of his or her right to access and to request corrections of his or her personal information, and how to do so;
d generally describe the security measures in place to protect personal information;
e inform individuals if personal information is transferred to foreign jurisdictions; and
f provide contact information for the organisation’s privacy officer or other person who can respond to inquiries about the organisation’s information handling practices.

The Privacy Commissioner also emphasises the value of augmenting privacy notices with other forms of notice, including ‘just in time’ notices (e.g., through pop-ups and interstitial pages) and layering notices to provide further information about more complex issues for those who seek such information and icons where applicable (e.g., the ‘Ad Choices’ icon for OBA).

In 2013, the Privacy Commissioner participated in the Global Privacy Enforcement Network Internet Privacy Sweep, which looked at privacy policies on 326 websites in Canada and 2,186 websites worldwide. The Commissioner noted concerns in almost half of the Canadian websites.25 In an example of ‘naming and shaming’, the Commissioner called out specific examples of privacy policies that he considered constituted the ‘good, the bad and the ugly of privacy policies’.26

**Principle 9 – individual access**

‘Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.’

Organisations are obliged to provide individuals with access to their personal information within a reasonable time frame. This obligation is subject to limited exceptions; for example, organisations may either be allowed or obliged to refuse access where disclosure would reveal personal information about another person; the information is subject to privilege, trade secrets or is confidential information; or the information pertains to law enforcement activity.

Organisations must also allow individuals to request corrections to their personal information. Where such corrections are refused (e.g., information is accurate), an organisation must make a notation on the individual’s file that a correction was requested as well as the reason for refusing the correction.

Organisations may charge a fee; however, fees must be reasonable.

**Principle 10 – challenging compliance**

‘An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organisation’s compliance.’

---


Organisations are required to designate a person who can respond to questions and complaints, and establish a process for responding to questions and complaints.

iv Technological innovation and privacy law

Privacy laws are intended to be ‘technologically neutral’, meaning the principles upon which they are based apply equally to all technologies.

However, one technology that has proven particularly challenging is OBA. After years of uncertainty about how Canadian privacy law applies to OBA,27 the Privacy Commissioner decided to address the issue by publishing its Policy Position on Online Behavioural Advertising (Policy Position).28

As described above, the Privacy Commissioner considers much of the information used for OBA purposes to be personal information. Thus, according to the Privacy Commissioner, PIPEDA (and other privacy legislation) applies to OBA.

The Policy Position is generally positive – it signals that the Privacy Commissioner is willing to accept some form of opt-out consent as sufficient for organisations that use OBA. This position is more lenient towards business interests in comparison to the strict opt-in approach adopted by the European Union.

The Office of the Privacy Commissioner (OPC) has adapted its opt-out consent framework to OBA, defining the following as a list of conditions:

- a individuals are informed about OBA in a clear and understandable manner at or before the time of collection;
- b organisations should rely on online banners, layered policies and interactive tools. Purposes must be obvious and cannot be ‘buried’ in privacy policies. This includes information about various parties involved in OBA (e.g., networks, exchanges, publishers and advertisers);
- c individuals can easily opt out, ideally at or before the time of collection;
- d the opt-out takes effect immediately and is persistent;
- e information is limited to non-sensitive information, to the extent practicable;29 and
- f information is destroyed as soon as possible or effectively de-identified.

27 For the purposes of this chapter, OBA refers generally to the delivery of advertisements to web browsers that are targeted based on a user’s behaviour online, and the collection, use and disclosure of data for those purposes.
29 In early 2014, the Privacy Commissioner found that Google had violated PIPEDA by using sensitive personal information to target and serve through its AdSense service. Google had allowed its customers to serve targeted adverts for Continuous Positive Airway Pressure devices to internet users identified as suffering from sleep apnoea. Although the Privacy Commissioner has stated that companies can rely on a form of opt-out, implied consent for OBA, adverts targeted at sleep apnoea sufferers did not qualify for this approach given that this involves the collection and use of sensitive, health-related personal information. See Privacy Commissioner of Canada, PIPEDA Report of Findings #2014-001 – Report of Findings: Use of sensitive health information for targeting of Google ads raises privacy concerns, 14 January 2014, www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2014/pipeda-2014-001.
Consistent with past guidance on the issue, the OPC emphasises the need for clear and understandable descriptions of OBA, given the challenges of clearly explaining such a complex issue.

The OPC has published research and guidance in recent years that considers the application of privacy law to other technologies and issues, including facial recognition, wearable computing, drones and genetic information.

v Specific regulatory areas

The implementation of CASL in 2014 was one of the most significant privacy-related developments in years. The law establishes rules for sending commercial electronic messages (CEMs) as well as the installation of computer programs, and prohibits the unauthorised alteration of transmission data.

CASL applies to most forms of electronic messaging, including email, SMS text messages and certain forms of messages sent via social networks. Voice and fax messages are excluded, as they are covered by the Unsolicited Telecommunications Rules. The law applies broadly to any CEM that is sent from or accessed by a computer system located in Canada.

A CEM is defined broadly to include any message that has as one of its purposes the encouragement of participation in a commercial activity. This includes advertisements and information about promotions, offers, business opportunities, etc.

CASL creates a permission-based regime, meaning that, subject to a number of specific exclusions, consent is required before sending a CEM. Consent can either be express or implied.

With respect to computer programs, CASL requires any person installing a computer program onto another person's computer system to obtain express consent from the owner or authorised user of the computer system.

CASL is enforced by the Canadian Radio-television and Telecommunications Commission (CRTC). The CRTC has the power to impose administrative monetary penalties for violations of CASL of up to C$10 million per violation.


IV INTERNATIONAL DATA TRANSFER AND DATA LOCALISATION

There are no restrictions on transfers of data outside Canada in private sector privacy legislation.\textsuperscript{34} PIPEDA requires organisations that transfer data to third parties for processing – whether inside or outside Canada – to ensure through contract that the protection provided is ‘generally equivalent’ to the protection that would be provided by the transferring organisation.\textsuperscript{35} With respect to the potential access to personal information by foreign governments and law enforcement agencies, the Privacy Commissioner has stated that while organisations cannot override or prevent such access through agreements, the law ‘does require organisations to take into consideration all of the elements surrounding the transaction. The result may well be that some transfers are unwise because of the uncertain nature of the foreign regime or that in some cases information is so sensitive that it should not be sent to any foreign jurisdiction.’\textsuperscript{36}

Although consent is not required for transfers to foreign jurisdictions, the Privacy Commissioner has interpreted PIPEDA to require organisations to advise customers (e.g., through privacy policies) that information may be transferred to foreign jurisdictions, and could therefore be accessed by government agencies there.\textsuperscript{37}

The Alberta Personal Information Privacy Act has more explicit requirements when transferring data to service providers outside Canada. Organisations that use service providers to process personal information outside Canada must:

\begin{itemize}
  \item[a] develop policies that describe the countries to which information is or may be transferred as well as the purposes for which the service provider may collect, use or disclose personal information, and make policies available upon request;\textsuperscript{38} and
  \item[b] provide notice to individuals that a service provider outside Canada will collect, use or disclose personal information, and provide information about who can answer questions and where the individual can obtain written information about policies with respect to transfers outside Canada.\textsuperscript{39}
\end{itemize}

V COMPANY POLICIES AND PRACTICES

Companies that do business in Canada are generally expected to have in place the following policies.

i General

Organisations should:
a establish detailed internal privacy policies for ensuring compliance with privacy legislation that address things such as who is responsible for compliance with privacy legislation;

b establish the various types of personal information collected, used and disclosed, and for what purposes;

c provide training for employees;

d establish administrative, physical and technical security measures for the protection of personal information;

e record transfers of personal information;

f record retention periods and the destruction of personal information;

g record the outsourcing of and third-party access to personal information;

h respond to requests for access to personal information;

i respond to inquiries and complaints about information handling practices; and

j identify and respond to security breaches.

ii Privacy notices

Organisations must have privacy notices for communicating privacy-related information to the public. This typically consists of an online privacy policy, but can be combined with other means such as written pamphlets, layered privacy notices and just-in-time notifications provided at the point of sale, online and in mobile applications.

iii Chief privacy officer

Organisations must establish a person who is responsible for compliance with privacy legislation. Further, privacy notices must provide contact information for a person who can respond to inquiries and complaints about information handling practices.

VI DISCOVERY AND DISCLOSURE

Privacy laws contain broad exceptions that allow organisations to respond to requests from government agencies for law enforcement purposes, such as in response to a subpoena or warrant, or in response to a court order in a civil proceeding. In addition, private sector organisations can disclose personal information on their own initiative in some circumstances.

There are also several laws that allow government agencies to collect and share information – including personal information – with foreign agencies. For example, the federal government has established bilateral and multilateral conventions for mutual legal assistance with several countries under the federal Mutual Legal Assistance in Criminal Matters Act.⁴⁰ Pursuant to these agreements, foreign governments can request information about a specific person, following which the Department of Justice Canada can apply to a court for a warrant compelling disclosure of the information.

⁴⁰ RSC, 1985, c 30.
There are also other laws that permit transfers to foreign agencies for specific purposes, including the Proceeds of Crime (Money Laundering) and Terrorist Financing Act, the Department of Immigration and Citizenship Act, and the Canadian Security Intelligence Service Act.

Foreign governments cannot directly compel an organisation located in Canada to disclose information. However, personal information about Canadians can be accessed by foreign governments once transferred to those jurisdictions. Canada does not have any ‘blocking statutes’ or specific procedures for resisting access by foreign governments to personal information about Canadians.

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

The Privacy Commissioner of Canada is responsible for the oversight and enforcement of PIPEDA. The Privacy Commissioner is an ‘ombudsman’, meaning that he or she can make recommendations to organisations, but cannot make orders or impose fines. Enforcement is primarily complaint-driven, although the Privacy Commissioner also has the authority to conduct investigations or audits on his or her own initiative. Either a complainant or the Privacy Commissioner can apply to the Federal Court seeking an order, an award of damages, or both. The Privacy Commissioner can also enter into compliance agreements with organisations if the Commissioner believes there has been, or is about to be, a contravention of PIPEDA. The Commissioner can also make public any information obtained in the course of his or her duties if doing so would be in the public interest.

Data protection authorities in Alberta, British Columbia and Quebec have the power to make enforceable orders, which are subject to appeal by provincial courts. Authorities in all jurisdictions (both federal and provincial) have powers to compel evidence.

Although damages are possible under private sector privacy legislation, damage awards are not common. One of the largest damage awards to date is C$20,000, which was awarded against Bell Canada for violating PIPEDA in 2013.

ii Private litigation

Privacy-related litigation has become more common in recent years, as courts are increasingly willing to recognise privacy as a compensable cause of action.

The following four provinces have established a statutory tort for invasion of privacy: British Columbia, Manitoba, Newfoundland and Labrador, and Saskatchewan. A common law tort for invasion of privacy was explicitly recognised for the first time in Ontario in 2012 in Jones v. Tsige. The court awarded relatively modest damages at C$10,000 in that case.

---

41 SC 2000, c 17.
43 RSC, 1985, c C-23.
44 Chitrakar v. Bell TV, 2013 FC 1103.
45 Privacy Act, RSBC 1996, c 373.
46 Privacy Act, RSM 1987, c P125.
47 Privacy Act, RSN 1990, c P-22.
49 2012 ONCA 32.
case, stating that damages for privacy invasions should be generally limited to a maximum of C$20,000. In a controversial 2017 decision, a small claims court in Ontario rewarded a plaintiff C$4,000 for intrusion upon seclusion.50 In 2016, the Ontario Superior Court cited a new tort referred to as the ‘public disclosure of embarrassing facts’ in a case arising out of the non-consensual publication of intimate images on the internet.51 The Court awarded damages of C$100,000, which is by far the largest award in a privacy-related case involving a single plaintiff to date.

There have been a growing number of data breach-related class actions in the past few years, involving defendants such as:

a. Home Depot;52
b. Bank of Nova Scotia;53
c. Human Resources and Skills Development Canada;54
d. Health Canada;55
e. Durham Region Health;56 and
f. Rouge Valley Health System.57

Although case law involving privacy breach class actions remains limited, precedents arising from class certification and settlement approval proceedings suggest that some courts are sceptical of class actions based on vague allegations of potential harm. For example, in the class action against Home Depot, the court reduced the fees to class counsel previously agreed by the parties, with the court stating that: ‘The case for Home Depot being culpable was speculative at the outset and ultimately the case was proven to be very weak.’58 However, settlements may be much higher where plaintiffs can provide more specific evidence of harm resulting from a breach.59

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

Organisations that collect, use or disclose personal information about Canadians are subject to Canadian law, regardless of their location. In response to a complaint about the collection, use and disclosure of personal information by a US-based data broker, the Privacy Commissioner determined that she did not have jurisdiction to compel the company to provide evidence. The Federal Court disagreed, finding that PIPEDA applied to the US data broker, and that the Commissioner did have jurisdiction to investigate because the

50 Vanderveen v. Waterbridge Media, 2017 ON SCSM 77435 (CanLii).
51 Jane Doe v. Waterbridge Media, 2016 ONSC 541.
54 Condon v. Canada, 2014 FC 250.
55 John Doe v. Her Majesty the Queen, 2015 FC 916.
57 No citations: Elia Brouzas and Meagan Ware v. Rouge Valley Health System, Jane Doe 'A', Jane Doe 'B'. John Doe Registered Savings Plan Corporation and Jane Doe 'C', Statement of Claim, CV-14-507026-00CP.
59 For example, in Evans v. The Bank of Nova Scotia, 2014 ONSC 2135 (CanLII), the defendant bank settled for approximately C$1.5 million as some class members suffered identity theft as a result of a data breach.
complainant was Canadian and much of the data had to come from Canada. The Court noted it was not required to find that PIPEDA applies extraterritorially to reach such a conclusion. It also stated that the fact that an investigation might be ineffective is irrelevant to the legal questions of jurisdiction.

IX CYBERSECURITY AND DATA BREACHES

Canada signed up to the Council of Europe’s Convention on Cybercrime in 2001, but is yet to ratify the treaty. Although there have been repeated attempts over the past decade to pass ‘lawful access’ legislation that would enable Canada to ratify the treaty, legislative proposals have been met with significant opposition. The key aspects of these proposals include new powers for production orders and preservation notices, and requirements that telecommunications service providers (TSPs) make their networks intercept-capable. In addition, proposals have included provisions that would allow law enforcement agencies to compel TSPs to provide customer name and address information without a warrant or court order, which have been most controversial. Mandatory data retention by TSPs has not been a feature of legislative proposals to date.

As of 1 November 2018, private sector companies subject to PIPEDA will be required to provide a report to the Privacy Commissioner and notify affected individuals of any breach of safeguards resulting in a real risk of significant harm (RROSH). Significant harm includes bodily harm, humiliation, damage to personal relationships or reputation, loss of employment or opportunity, financial loss, and identity theft.

In assessing a RROSH, an organisation would have to consider the sensitivity of the information involved and the probability that the information will be misused.

X OUTLOOK

Privacy-related litigation will continue to grow and should be a top priority for organisations doing business in Canada. While the government has yet to set a schedule for implementing the recommendations listed in the 2017 statutory review of CASL, its positive response to the review’s recommendations should be noted – particularly in regards to clarifying issues surrounding the Act’s interpretation. Given the review’s recommendations, it appears that the private right of action under CASL will continue to be delayed until the government clarifies the more pressing provisions of CASL.

Organisations should also be cognisant that data breach notification requirements under PIPEDA are in effect of 1 November 2018.

---

Chapter 9

CHINA

Marissa (Xiao) Dong

I OVERVIEW

China does not have an omnibus data protection law as such. In 2005, some legal scholars published a discussion draft for a PRC data protection law, which was reportedly the basis for the State Council draft. However, to date, the State Council has not published the draft data protection law. In fact, data protection law is not included in the 12th National People’s Congress (NPC) legislative plan, which applies to the period 2013–2018.¹

Despite the lack of a unified law, China currently has a system of legal rules in place in relation to the protection of personal information, albeit a complicated system. In 2012, the Standing Committee of the NPC issued the Decision on Strengthening Internet Information Protection³ (the NPC Decision), which requires enterprises and, in particular, internet service providers, to protect the personal electronic information of Chinese citizens with several general principles. Following the NPC Decision, a sector-specific legal regime in respect of personal information has gradually formed in China, with various departments of the State Council such as the Ministry of Industry and Information Technology (MIIT), the State Administration for Industry and Commerce (SAIC), the National Health and Family Planning Commission (NHFPC) and the People’s Bank of China (PBOC) respectively issuing personal protection rules under their own administrative authority over the past few years, and in some circumstances these have overlapped. In the absence of a unified legal definition, ‘personal information’ is defined under many industry-specific rules and generally refers to the information relating to an individual that, alone or in combination with other information, can be used to identify an individual. All these regulations and rules have identified a number of general principles for processing personal information (e.g., personal information collection should follow the principles of legitimacy, appropriateness and necessity, and should be subject to the relevant individual’s consent).

The issuance, on 7 November 2016, of the Cybersecurity Law of the PRC (CSL) is also considered a milestone. The CSL, which became effective from 1 June 2017, includes provisions relating to both cybersecurity protection obligations and data privacy obligations.

If an individual’s right to privacy is infringed, the individual may bring a civil lawsuit against the injuring party to seek redress under the Tort Liability Law. Further, sale of personal information or illegal acquisition of personal information may constitute a criminal offence.

¹ Marissa (Xiao) Dong is a partner at Jun He LLP. Passages of this chapter were originally published in ‘Data Protection Considerations for Commercial Arrangements between the EU and China’, August 2013, and ‘Data Privacy and Security Law Develops Quickly in China’, August 2015
² See www.gov.cn/jrzg/2013-10/30/content_2518276.htm.
³ See www.gov.cn/jrzg/2012-12/28/content_2301231.htm.
From a legal point of view, China's personal information legal system is still far less effective and robust than that of the United States or of the EU. It has also long been debated in China whether, in terms of legislation and practice, the country should follow the route of the United States or of the EU. While learning from both models, China has not yet committed to one or other of these approaches, and in fact the Chinese way, as it has been formed in practice, is somewhat of a mixture of both. With a view to cracking down on the serious abuse of personal information, Chinese legislators have introduced a broader scope of personal information offences in the recently promulgated amendment to the Criminal Law. Furthermore, in judicial practice, in a recent civil case, *Ms Zhu Ye v. Baidu*, the Chinese court ruled that the use of cookies by internet service providers, and accordingly delivering targeted advertising, does not violate the right of privacy of Chinese citizens, which has been read by the press as a judgment in favour of the ‘new economy’. Chinese companies and multinationals in China are gradually paying more attention to their practice of collection and utilisation of personal information in China, with some promoting industry-specific standards to provide guidance in the still comparatively grey areas.

In brief, although from an overall perspective the abuse of personal information is still a very serious reality, and people living in China still suffer unsolicited calls, emails and text messages, the attitude and rules of the governmental authorities, the practice of companies, the understanding of courts and, more importantly, public awareness are changing in a fast and sometimes dramatic fashion in this information era, which is unlike anything that any other nation, or even the world, has previously experienced.

II  THE YEAR IN REVIEW

More national standards relating to cybersecurity protection in various industrial and niche areas are being released for public comment, while many of the drafts that were previously issued for public comment by regulators are still pending in 2018. Such drafts include the Measures on Security Assessment of the Cross-Border Transfer of Personal Information and Important Data, and the Regulations on Security Protection of Critical Information Infrastructures, which have attracted wide attention from the market. Yet government agencies have become more active in enforcing the CSL and relevant regulations already effective, especially in the area of cybersecurity protection and crimes relating to the illegal sale and acquisition of personal information. Companies have become more alert to compliance in this area, and have gradually started programmes to evaluate, prepare and strengthen internal control over cybersecurity and personal information protection. The skeleton of the new legal regime in China is gradually being built, though many specific requirements, procedures and details are to be inserted and are expected in the market.

III  REGULATORY FRAMEWORK

China's regulatory framework for personal information protection includes laws and regulations in the criminal, civil and administrative areas.

i  Privacy and data protection legislation and standards

*CSL*

The CSL provides various security protection obligations for network operators, including, *inter alia*:
China

a compliance with a series of requirements of tiered cyber protection systems (Article 21);
b verification of users’ real identity (an obligation for certain network operators) (Article 24);
c formulation of cybersecurity emergency response plans (Article 25); and
d assistance and support to investigative authorities where necessary for the protection of national security and investigation of crimes (Article 28).

The CSL, for the first time under PRC law, clearly imposes a series of heightened security obligations for critical information infrastructure operators (CIIOs), including:

a internal organisation, training, data backup and emergency response requirements (Article 34);
b storage of personal information and other important data must be secured within the PRC territory, in principle (Article 37);
c procurement of network products and services that may affect national security must pass the security inspection of the relevant authorities (Article 35); and
d annual assessments of cybersecurity risks and reports on the results of those assessments and improvement measures to be submitted to the relevant authorities (Article 38).

As regards personal information, the CSL reiterates the obligations of network operators regarding the protection of personal information that appear across existing laws and regulations, including the mandate to observe the principle of lawfulness, necessity and appropriateness in the collection and use of personal information and to observe the ‘inform-and-consent’ requirements (Article 41), to use personal information only for the purpose agreed upon by the relevant individual (Article 41), to adopt security protection measures for personal information (Article 42), and to protect the individual’s right to access and correct personal information (Article 43). In addition, the CSL also incorporates some new rules on personal information protection, including data breach notification requirements (Article 42), and data anonymisation as an exception for inform-and-consent requirements (Article 42), and the individual’s right to request that network operators make corrections to or delete their personal information if the information is wrong or used beyond the agreed purpose (Article 43).

Criminal offence

Article 253 of the Criminal Law (as provided in Amendment VII to the Criminal Law)4 applies where any individual (including staff of governmental authorities and companies engaged in industrial sectors, including finance, telecommunications, transportation, education and healthcare) sells or illegally provides personal information obtained in his or her employment and where the circumstances are ‘serious’. It is also applicable if an individual illegally acquires such information by stealing or by any other means and where the circumstances are serious. Legal consequences of such acts include fixed-term imprisonment of up to three years, criminal detention or fines. In the event that an entity commits either of these crimes, the entity is subject to a fine, and the individual in charge and other individuals directly responsible for the criminal activity are subject to the punishments listed above.

Amendment IX to the Criminal Law,\(^5\) which became effective from 1 November 2015, has amended Article 253, and has broadened the scope of personal information-related offences and increased legal liability.

The Supreme People’s Court and the Supreme People’s Procuratorate also promulgated the Interpretation by the Supreme People’s Court and the Supreme People’s Procuratorate on Issues Concerning the Application of Law in Handling Criminal Cases of Infringing on Citizens’ Personal Information and relevant typical cases, effective from 1 June 2017, providing more details as to how Article 253 should be interpreted and implemented.

**Tort liability**

The Tort Liability Law,\(^6\) effective as of 1 July 2010, includes many provisions that specifically or generally relate to the protection of personal data, and in particular, in Article 2, defines the ‘civil rights and interests’ protected under the Law, specifically listing 18 types of right and including the right of privacy. This is the first time under PRC law that the right of privacy has been treated as an independent type of civil right, and no longer attached to the right of reputation. Under the Tort Liability Law, the violation of the right of privacy and other personal and property rights and interests is clearly provided as constituting a tort. An injured party can seek redress against the injuring party.

**Industry-specific regulations and rules**

The NPC Decision, as mentioned above, has set forth a number of important principles for handling personal electronic information. It is also important to note that the Consumer Rights Protection Law,\(^7\) effective as of 15 March 2014, includes and echoes the requirements of the Decision.

Accordingly, various governmental authorities have issued their respective administrative regulations and rules to set out more specific requirements in their area – including, for example, MIIT, SAIC, NHFPC – and to provide rules for a number of different types of personal information. For example:

- Users’ personal information collected by telecom and internet operators in their business operations;
- Operators’ and users’ personal information collected in the course of e-commerce platforms’ business; and
- Population health information collected by healthcare organisations and entities.

**General obligations for data handlers**

In brief, data handlers generally have to obey the following principles:

- Complying with the principles of lawfulness, fairness and necessity when collecting and using personal information;
- Informing data subjects, explicitly, of the purpose, methods, scope of the collection and use of personal information, and obtaining their consent;
- Publishing statements describing the collection and use of data subjects’ personal information;

---

keeping personal information strictly confidential, and refraining from disclosing, selling or illegally providing such information to others;

taking necessary measures to ensure the security of personal information and, in the event of the disclosure or loss of such information, immediately take remedial measures; and

refraining from sending any commercial messages to an individual without his or her consent or request, or if the individual has expressly refused to receive such information.

iii Technological innovation and privacy law

Chinese law does not generally prohibit the use of online tracking and behavioural advertising, cloud computing and big data, and as mentioned in Section II, the government is actively promoting such technological innovation in China to facilitate growth in the industry. Nevertheless, many issues still lack clarity under the law, and this legal ambiguity has, in practice, brought about uncertainty for business operators, particularly where the adoption of new types of technology or business model are concerned.

Cookies

The use of cookies is a good example of the above-mentioned issues, and there have been contradictory views around key aspects of the use of cookies. On 15 March 2013, World Consumer Rights Day, the Chinese Central Television Station specially reported that consumers’ personal information was being divulged when they surfed the web, and accused many websites of prying into internet users’ privacy.8 The report caused widespread public panic. Although many industry participants sought to clarify the facts around the use of cookies, many people were still not clear about how cookies work exactly and whether indeed their privacy had been invaded. From a legal point of view, many issues are not clear because of the lack of detailed rules. For example, the specific reference of the consent requirement for the purpose of utilising the personal information of individuals is not clear under certain circumstances, whether implied consent is sufficient in all scenarios, or to what extent business operators must disclose to users or consumers details of proposed future use of information collected. The Chinese Advertising Association is actively promoting industry standards for targeted advertising and mobile internet advertising,9 and it is still waiting to see whether these standards will be widely accepted and implemented in practice.

In the first civil case regarding internet advertising and the online collection and use of personal information, involving Chinese search engine giant Baidu, a Ms Zhu claimed that Baidu’s targeted advertising on its partners’ websites, using cookies set when she used the search engine, infringed her right to privacy. Interestingly, the appellate court’s judgment contrasted with the opinions of the court of first instance in many aspects. The appellate court decided three important points at variance with the judgment of the court of first instance: that the information collected by Baidu cookies does not contain personal information under PRC law; that the network user does not suffer cognisable injury by receiving targeted adverts on websites within Baidu’s advertising alliance; and that the notification and consent

---

8 See finance.qq.com/a/20130315/007380.htm.

© 2018 Law Business Research Ltd
mechanism provided on Baidu’s search engine website is legal and sufficient. Although the Chinese court judgment does not have a binding effect, it provides important guidelines and may affect other similar cases in the future.

**Cloud computing**

Cloud computing has posed new challenges to the law, in particular because it is not completely transparent as to where and how the information is stored and processed in ‘the cloud’, or how prevention of hacker attacks and the security of information stored in the cloud may be assured. As mentioned in the Opinions for Promoting Creative Development of Cloud Computing and Fostering a New Sector of Information Industry issued by the State Council, China is faced with various issues with respect to cloud computing, along with development opportunities. These issues include lack of service capacity and core technology, insufficient sharing of information resources and high levels of information security risk. In the Opinions, the State Council’s demands include:

- facilitating research into applications of personal and enterprise information in a cloud computing environment;
- promulgation of laws and systems relating to information protection;
- rules relating to collection, storage, transfer, deletion and international transfer of information; and
- information security law.

**iv Specific regulatory areas**

Many different specific types of personal information are governed under different sets of laws and administrative rules, and some of these provisions overlap. A few common types of personal information are listed below.

**Users’ personal information in telecom and internet services**

‘Users’ personal information’ in telecom and internet services is defined under the Provisions on the Protection of Personal Information of Telecommunications and Internet Users (the Protection Provisions) of July 2013. The Protection Provisions stipulate several measures that telecommunications and internet service providers should take internally for the prevention of leakage, damage or loss of personal information of users. The Protection Provisions also provide that telecommunications authorities should check how telecommunications and internet service providers protect personal information during the annual inspection in respect of their telecommunications licence.

**Population health information**

‘Population health information’ is stipulated under the Administrative Measures for Population Health Information (for Trial Implementation), effective on 5 May 2014, as information generated and collected in the course of service and administration by medical, healthcare and family planning services agencies. The collection and handling of population health information is subject to specific rules, and such information is particularly prohibited from being stored outside China.

10 See www.gov.cn/gzdt/2013-07/19/content_2451360.htm.
11 See www.gov.cn/gzdt/att/att/site1/20131119/7845c441d9c213f568c201.doc.
Personal financial information

Financial institutions, including banks, insurance companies, securities companies and similar organisations, are required to preserve client information that they obtain in the course of business operations under the Administrative Measures Regarding the Retention by Financial Institutions of Customer Identification Documents and Materials and Transaction Records. Financial institutions in the banking industry are subject to more specific requirements under the Notice of Strengthening the Work Relating to the Protection of Personal Financial Information by Financial Institutions in the Banking Industry issued by the PBOC. ‘Personal financial information’ is defined as information that is obtained, processed and retained by financial institutions during their business operations, or through their access to the credit information system of the PBOC, payment systems and other systems that include:

a) personal identification information;
b) information pertaining to personal property;
c) information pertaining to personal accounts;
d) personal credit information;
e) information pertaining to personal financial transactions;
f) derived information, such as personal consumption habits and investment intentions, which can reflect certain situations of the individual and are formed by handling and analysing the relevant raw information; and
g) other information obtained and preserved during the course of establishing a business relationship with the relevant individual.

IV INTERNATIONAL DATA TRANSFER AND DATA LOCALISATION

Although at present there are no specific legal requirements for the transfer of personal information within China itself, the cross-border transfer of personal information from China to other jurisdictions is subject to the general privacy requirements under civil law. Where the personal information to be transferred is of a specific nature, there are also explicit requirements under industry-specific regulations and rules.

For example, in the heavily regulated banking industry, the processing of personal information collected by commercial banks is administered by stringent rules. The PBOC especially requires that personal financial information collected in China must be stored, handled and analysed within the territory of China and, unless otherwise stipulated, banks are not allowed to provide domestic personal financial information overseas. Another example is the transfer of employee information, which is very sensitive in practice and requires delicate handling despite the provisions regarding employee information being comparatively simple at present.

In addition to stipulations under civil law and industry-specific regulations, disclosing information to an offshore entity is strictly prohibited if the information involves PRC state secrets. This issue has become highly sensitive where Chinese subsidiaries of US companies and companies listed in the United States are requested to provide information to the US authorities or US affiliates in relation to internal Securities and Exchange Commission investigations, or where foreign companies are conducting internal investigations (e.g., for

---

13 See www.gov.cn/gongbao/content/2011/content_1918924.htm.
Foreign Corrupt Practices Act purposes) and their Chinese subsidiaries need to transfer documents overseas. Under the State Secrets Protection Law (2010)\textsuperscript{14} and the Measures for Implementing the State Secrets Protection Law (2014),\textsuperscript{15} no documents or materials containing state secrets are allowed to be carried, transmitted, posted or transported outside China without approval from the competent governmental authorities. However, the term ‘state secrets’ is broadly defined, covering extensive matters such as major decisions on state affairs, national defence and activities of the armed forces, diplomatic activities and foreign affairs, national economic and social development, science and technology, activities safeguarding national security, and the investigation of criminal offences. The lack of an explicit list or guidelines specifying what information constitutes state secrets, or procedures to recognise state secrets, have contributed, in practice, to extreme difficulty in dealing with information that might be considered as containing state secrets.

Furthermore, the Information Security Technology Guide for Personal Information Protection within Information Systems for Public and Commercial Services\textsuperscript{16} (the Guidelines) was issued on 15 November 2012, and became effective from 1 February 2013. The Guidelines, however, do not serve as a statutory law but as a non-mandatory national standard. Nevertheless, as many important internet service providers have been participating in the process of their drafting, the Guidelines are expected to be observed, or at least used as reference in establishing internal rules, by many industry participants, and some believe the Guidelines may serve as a basis for future legislation on personal information protection. The Guidelines set out both general principles and specific requirements with respect to the collection, processing, transmission, utilisation and management of personal information in various information systems. In particular, in respect of cross-border transfers of data, the Guidelines provide that in the absence of explicit law or regulation, and without the approval of the industry administrative authority, a Chinese data controller should not transfer any personal information to a data controller registered overseas. Although this recommendation is not mandatory, it reflects the attitude of the governmental authorities that have participated in the issuance of the Guidelines, and we would expect there may be increasingly strict legal requirements in this regard in the future.

Notably, CAC released a draft of the Measures on Security Assessment on the Cross-Border Transfer of Personal Information and Important Data for public comment and it has yet to be finalised. The Draft requires, in addition to the data localisation and security assessment on CIIOs, that all ‘network operators’ should also carry out security assessments for cross-border transfers of personal information and important data collected and produced by them in the course of their operations within China. The Draft regulates cross-border data transfers by way of both ‘self-assessment’ and assessment by authorities. In brief, network operators are required to carry out self-assessment for all cross-border transfers of data, while cross-border transfers of data satisfying certain tests must be submitted to the applicable industrial regulatory authority or the national cyberspace authority for assessment.

The National Information Security Standardisation Technical Committee (TC 260) released a draft of the Information Security Technology Guidelines for Cross-Border Data Transfer Security Assessment for public comment (and a second draft has already been released). As an important ancillary document to the CSL, the Guidelines put forward detailed

\textsuperscript{14} See www.gov.cn/flfg/2010-04/30/content_1596420.htm.
\textsuperscript{15} See www.gov.cn/zwgk/2014-02/03/content_2579949.htm.
\textsuperscript{16} See tech.qq.com/a/20110211/000264.htm.
recommendations on the assessment process, assessment methods and points regarding the data export security assessment. Although the Guidelines do not have mandatory legal force, they may be adopted and referred to in data export activities by network operators in various industries, since existing laws and regulations fail to provide detailed guidance. In data export assessments, enterprises need to comprehensively take into account factors such as the consent of the individuals whose personal data is being exported, the necessity for the data export, the security protection measures of the data exporters and data recipient, and the political and legal environment of the receiving country or region.

V COMPANY POLICIES AND PRACTICES

Following the entry into force of the CSL in China, companies have started to consider and adopt rules for the collection and processing of information obtained both in the course of their business and from their employees' personal information, and also rules regarding their cybersecurity protection practices.

Under the CSL, it is provided that a CIIO must designate a person with specific responsibility for security management organisation and security administration, and carry out a security background check on that responsible person and on relevant personnel holding key positions. Network operators are required to appoint personnel responsible for cybersecurity protection. Although not specifically mentioned, telecom and internet service providers are required to set up a security officer post, and they are also required by the MIIT to specify the responsibilities of each department, post and branch in terms of managing the security of users' personal information, and to establish work processes and security management systems for the collection and use of users' personal information and related activities.

VI DISCOVERY AND DISCLOSURE

In practice, discovery and disclosure issues mainly arise out of cases involving cross-border investigations or litigation. For example, a subsidiary of a US company in China may be required to produce documents when the US company is ordered to produce information on the basis of a subpoena, or a Chinese company may also be subject to such a requirement if the company is sued in the United States. There will be complex state secret and personal information issues involved in the discovery and disclosure process, and a Chinese lawyer's legal opinion is normally sought to ensure that the process is carried out in compliance with PRC law. Again, because of the lack of explicit rules, such a process can be challenging and tricky, and may involve communication with different Chinese governmental authorities. Cross-border transfer requirements pursuant to the CSL will also need to be taken into consideration.

VII PUBLIC AND PRIVATE ENFORCEMENT

China does not have a central privacy regulator, and many governmental authorities regulate privacy issues within their own delegated area of authority (normally a specific industry sector), and these areas may overlap. For example, the MIIT is in charge of telecom and internet service providers, the SAIC administers market order, consumer rights protection and advertising issues, and the PBOC is in charge of the administration of personal financial
information. Although there have been sanctions imposed by the SAIC and the PBOC in certain localities for the leaking or abuse of personal information, there have been no milestone cases yet. CAC is the designated enforcement authority for the CSL and following the entry into effect of the CSL it has already been active, starting investigations into practices in this area.

There have already been various privacy lawsuits, even before the Tort Liability Law became effective, and at that time claims were brought for infringement of the right to reputation. However, there is still no unified interpretation of what constitutes privacy of individuals and what circumstances would be treated as infringements of privacy rights. Although many judgments rendered by local courts have provided their views and guidance on this matter, these cases are not legally binding. There are still controversial views held by different local courts on this matter.

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

Strictly from a legal point of view, the rules for handling personal information only apply to businesses operating within Chinese territory. However, in this high-tech era, the boundaries of business blur, and sometimes it is unclear and uncertain how these rules would apply, in particular when, as is the case on many occasions, cross-border business such as e-commerce is involved. Foreign organisations operating on the internet in a Chinese market and with Chinese customers as their main target would still have to consider whether they are required to set up a presence in China as a first step for the business and, subsequently, whether they would need to follow Chinese data protection rules. The CSL and its ancillary rules, in particular the draft measures and guidelines for cross-border data transfer, will also pose new challenges for foreign organisations with operations in China.

IX CYBERSECURITY AND DATA BREACHES

In April 2014, to respond to the various challenges in the new era, President Xi Jinping for the first time raised the ‘overall concept of national security’. Thereafter, a series of pieces of legislation relating to national security was put on an accelerated track, including the National Security Law (NSL), the Counter-Terrorism Law (CTL) and the CSL. The CTL, NSL and CSL all include, or are likely to include, provisions relating to information and technology security, and have drawn wide attention from foreign companies, especially high-tech and internet companies that have operations in China.

On 1 July 2015, China’s legislature, the NPC Standing Committee, passed the NSL, and it came into effect on the same date. The NSL, for the first time, provides for ‘safeguarding the national cyberspace sovereignty’, and adds cybersecurity and information security as important parts of national security, in contrast with the former NSL, which focused primarily on counter-espionage. The NSL further requires the state to establish a national security review system to review matters and activities that influence or may influence national security, including those relating to network information technology products and services.

The CTL was enacted at the end of 2015. The CTL is the first counter-terrorism law in China that includes wide-ranging stipulations and is intended to cover to all aspects of counter-terrorism activities. The CTL provides, *inter alia*, obligations for telecom and internet enterprises to cooperate with government authorities in investigating terrorism...
activities, which may have a significant impact on the operation of internet and tech firms in China. For example, according to the CTL, telecom and internet service providers are required to provide technical interfaces and technical assistance in decryption and other efforts to public and national security authorities engaged in the lawful conduct of terrorism prevention and investigation. However, the provisions of the CTL still lack details as to how these requirements will be implemented, which remains to be seen in practice.

As mentioned above, the CSL entered into effect on 1 June 2017 and has become the fundamental law in China for the protection of cybersecurity and personal information.

X OUTLOOK

As with the rest of the world, in China, threats to cybersecurity have been the subject of more intense focus by governmental authorities and public and private companies. Over the past few years, there has been an increase in China in the amount of legislation regarding personal information protection and cybersecurity law, and how these new laws and regulations will be implemented remains to be seen.

The CSL is considered a legislative milestone in China in this field. The CSL is the first law in the PRC specially focused on cybersecurity matters. With the entry into effect on 1 June 2017 of the CSL, internet companies and other industries in China are now subject to a wide array of stricter, more comprehensive obligations, and face more severe punishments for violations. As an omnibus law on cybersecurity issues, the CSL has many provisions that are still very general and abstract, and the detailed requirements for implementation and enforcement depend on subsequent and more specific implementation regulations, and on opinions from relevant authorities. We can expect the relevant regulatory authorities to continue to promulgate series of implementation regulations to clarify certain requirements under the CSL, such as regulations on tiered cybersecurity protection systems, the specific scope and protection measures regarding CII, the protection of minors on networks, the mandatory security certification and the test requirements for key network devices and special cybersecurity products, and national security reviews of the network products and services procured by CIIOs.

In view of these legislative changes, companies will have to consider whether they need to adjust their business operations and practices accordingly and enhance their cybersecurity protections to ensure full compliance with the CSL. Given that the specific details of implementation of the CSL requirements are not yet entirely clear, companies will also have to follow closely any subsequent releases of regulations and opinions by the relevant governmental authorities. In the year ahead, companies are also looking forward to seeing new regulations, standards and movement by the Chinese regulators, and how the draft regulations and standards are to be issued and implemented in practice.
I OVERVIEW

Article 15 of the Colombian Constitution of 1991 sets forth the fundamental rights of every individual to intimacy and privacy. Furthermore, Article 15 acknowledges the right to know about, update and rectify personal information that has been collected in public or private databases. This right is considered to be a development of the right to intimacy and a dimension of individual freedom, and is widely known as the habeas data right.

Until 2008, the scope of the habeas data right was developed mostly by constitutional case law and some activity-specific regulation, but there were no general or industry-specific laws regarding the matter. In 2008, Congress enacted Law 1266, with the main purpose of regulating use of financial and commercial personal data and, particularly, the use of financial, credit and commercial data used with the purpose of credit scoring. The right developed by Law 1266 is known as financial habeas data.

More recently, in 2012, Congress enacted Law 1581 with the purpose of establishing a more comprehensive legal framework, applicable to almost all commercial, non-commercial and governmental activities. Law 1581 determines the definitions and principles that govern data processing, establishes the rights of data subjects and duties of data controllers and processors, sets forth requirements for international data transfers, creates the National Registry of Databases and designates the Superintendence of Industry and Commerce (SIC) as the data protection authority, among others.

Colombian data protection regulation is inspired and follows the principles of the European data protection regulation. However, Colombian data protection law is highly focused on consent and provides few exceptions to the general rule that all processing must be authorised by the data subject.

Before Law 1266 of 2008 and Law 1581 of 2012, few Colombian organisations were aware of the need to adopt measures to protect personal information or had implemented an organisational culture around privacy. Since the enactment of these laws, both public and private entities have begun the process of aligning formally and substantially with the requirements of the law. However, it is important to take into account that many aspects of the law and regulation remain unclear and are being still developed by the data protection authority, controllers and processors.
II THE YEAR IN REVIEW

During the last year, Colombia has continued to develop guidelines and deepening the authorities positions on data protection.

On 10 August 2017, SIC issued Circular No. 5, a binding instructions guideline that establishes the criteria to determine if a country has adequate levels of data protection and provides a list of the countries that comply with such criteria. According to the law, international transfer to these countries is permitted. The first drafts of the Circular initially excluded the United States from the list but, after considerable public and academic discussion, the United States was finally included within the list of countries to where international data transfer is permitted.

Also, on 18 January 2018, the Ministry of Commerce, Industry and Tourism issued Decree 90 of 2018, that modified some aspects related to the National Registry of Data Bases. Decree 90 extended the term that companies have to register databases in the National Registry of Databases, and established a new threshold in order to limit registration to companies that have assets over approximately US$7 million.

Regarding new investigations, Colombia was one of the countries that took action related to the Cambridge Analytica global scandal. In March 2018, owing to possible links with Cambridge Analytica, SIC opened an investigation against the companies Farrow Colombia SAS (Colombia) and Farrow Mexico Sapi De CV (Mexico), that administered the application Pig-gi-2. SIC also ordered the temporary blocking of the application as a precautionary measure while the investigation was carried out.

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

The Colombian privacy and data protection legislation and standards are contained mainly in:

a Article 15 of the Colombian Constitution;
b Law 1266 of 2008 (financial privacy rules) and Law 1581 of 2012 (general privacy rules), together with the corresponding regulatory decrees; and

c instructions and guidelines issued by SIC, the data protection authority.

ii Principles

Law 1581 sets forth the main principles applicable to the processing of data, as follows:

a Legality: data processing is a regulated activity that must comply with the law and applicable regulation.
b Purpose: all processing must have a legitimate and constitutional purpose that has been notified to the data subject.

2 Later amended by Circular 008 of 2018, to include Japan in the list of countries that have adequate levels of data protection.
4 Law 1581, Title II, Article 4.
c Freedom (consent): personal data may only be processed after acquiring prior, express and informed consent from the data subject. Personal data may not be obtained or divulged without prior authorisation, or without a legal or judicial mandate that exempts processing from consent.

d Veracity or quality: information subject to processing must be truthful, complete, exact, updated, demonstrable and comprehensible. The processing of partial, incomplete or fractioned data that may be misleading is prohibited.

e Transparency: controllers and processors must guarantee data subjects the right to obtain information regarding all data that concerns him or her, at any time and without restriction.

f Restricted access and circulation: processing is subject to limitations imposed by the nature of the data and constitutional and legal provisions. Processing may only be carried out by persons authorised by the data subject or the persons permitted by law. Except for public information, personal data should not be available in the internet or any other massive communication or dissemination media, unless the access is technically controlled to provide access only to data subjects or authorised third parties.

g Security: data processing requires the adoption of all technical, human and administrative measures that are necessary to provide security and avoid unauthorised or fraudulent adulteration, loss, consult, use or access of the data.

h Confidentiality: everyone who intervenes in the processing of personal data not classified as public, is required to guarantee the confidentiality of the information.

ii Definitions

Law 1581 sets forth the following definitions:

a Controller: a natural person or legal entity, private or public, that decides the database and the processing of the data, whether by itself or together with third parties.

b Processor: a natural person or legal entity, private or public, that performs processing on behalf of the controller, whether by itself or in association with others.

c Personal data: any information linked or that may be associated with one or more determinate or determinable natural person.

d Database: an organised set of data that is the object of processing.

e Data subject: a natural person whose data is the object of processing.

f Processing: any operation or set of operations regarding personal data, such as collection, storage, use, circulation or suppression.

iv Classification of data

Data privacy laws provide the following classification of data.

Public data

Personal data that is not semi-private, private or sensitive. Among others, the following data is considered to be public: data related to marital status, profession, qualification as a merchant or public servant, etc. Because of its nature, public data may be contained, among others, in public records, official bulletins or judicial decisions (not sealed).

Private data

Data that is only relevant to the data subject owing to its intimate and confidential nature.
**Sensitive data**

Data that affects the intimacy of the data subject or that has the potential of generating discrimination against the data subject when unduly used. Examples of sensitive data is that which reveals the racial or ethnic origin of the data subject, his or her political orientation, religious or philosophical convictions, participation in unions, human rights organisations or political parties, as well as those data related to health, sexual health or biometric data.

**Semi-private data**

Data that does not have an intimate, confidential or public nature, and knowledge or publishing of which interests not only the data subject but also a group of people or society in general.

**ii General obligations for data handlers**

According to the data protection regulation, data controllers must comply with the following general obligations:

a warrant the data subject its absolute and effective right to *habeas data*, at all times;
b request and keep a copy of each signed authorisation granted by the data subject;
c inform the data subject of the purpose of the data collection;
d store all information under the security conditions necessary to prevent it from being tampered with, lost or disclosed or accessed without authorisation;
e warrant that the information supplied to the processor is true, complete, accurate, up to date, verifiable and understandable;
f rectify the information when found to be inaccurate and inform the processor as necessary;
g demand processors adopt security and privacy conditions to safeguard the data subject’s personal information;
h process data subject’s requests and complaints within the mandatory legal terms;
i adopt an internal manual of policies and procedures in order to guarantee adequate compliance with the law; and
j inform the data protection authority when data breaches occur.

Although Law 1581 was passed almost seven years ago and many organisations and entities began complying with the law, it was not until a couple of years ago that most organisations started implementing a real culture around data protection. This change was fostered by the obligation to register databases in the National Registry of Databases, which requires companies to assess and declare the level of compliance with the law.

Furthermore, the legislation establishes that data subjects will be entitled to:

a know, update and rectify their personal data with data controllers and processors. This right may be exercised, *inter alia*, relating to partial, inexact, incomplete, fragmented and misleading data, or whose processing is explicitly forbidden or has not been authorised by law;
b request proof of the authorisation granted to the data controller;
c be informed by the data controller about the use made of their personal data;
d file complaints with the Superintendence of Industry and Commerce for violations of the data protection regulation;
e withdraw the authorisation, or request data suppression when the data processing fails to comply with the principles, rights and legal and constitutional guarantees. The
withdrawal or suppression will proceed when the Superintendence of Industry and Commerce determines that the data controller or data processor has acted against this law or the Constitution;

f) access, free of charge, their personal data being processed; and

g) if they believe a processor or controller is not respecting their rights or complying with the law, file a complaint with the Superintendence of Industry and Commerce, which may admonish the controller or processor, or decide to open an administrative investigation.

iii Specific regulatory areas

Although Law 1581 establishes the general regime applicable to most activities and industries, it expressly excludes processing of financial privacy matters, which is regulated by Law 1266 of 2008.

Law 1266 regulates data processing for the purposes of calculating credit risk, and establishes rights and duties for sources, operators and users of financial data related to monetary obligations.

Furthermore, Colombian law includes specific privacy provisions and rules applicable to certain sectors or activities, and which apply concurrently with the general regime. Regarding children’s privacy, for example, Law 1581 sets forth special treatment for such data, and the privacy protection authority has issued a guideline specific to public and private education institutions. Also, there are sector-specific rules and case law related to the health sector (specifically, the social security system and medical history), and related to employment relationships.

iv Technological innovation

Regulatory framework

Law 1581 does not include a specific regulatory framework for privacy issues created by technological innovation. However, its principles and rules apply to any activity related to the use of personal data, including those activities related to online tracking, behavioural advertising, location tracking, use of cookies, profiling, etc.

In our opinion, the strict consent-driven approach of Law 1581 may unfortunately disincentivise technological innovation, owing to the constant change of purposes and uses that technological advances entail, which are sometimes difficult to foresee at the moment when consent is collected from the data subject.

Biometric data

It is important to note that Law 1581 specifically classifies biometric data (which includes facial recognition data) as ‘sensitive’ data, and provides specific requirements to acquire consent to use such data.

---

5 Article 7, Law 1581 of 2012.
6 See, for example, Resolution No. 1995 of 1999 of the Ministry of Health, Decisions C-264 of 1996 and T-1105/05.
7 See, for example, Decisions T-768/08 and T-405/2007 of the Constitutional Court.
Cloud computing
In 2015, SIC issued a guideline for using cloud computing according to the data protection regulation. This guideline establishes special recommendations for clients and providers when hiring or offering cloud computing services.

Big data
The National Council for Economic and Social Policies (CONPES), has recently issued a paper\(^8\) that recommends that the government makes a plan of action in order to: (1) increase the availability of data of public entities in order for the data to be accessible, usable and of quality; (2) provide legal certainty for the mining of personal data; (3) increase the available qualified professionals to process data; and (4) generate a data culture in the country.

Regarding the legal framework, the CONPES recommends that the country creates a better classification of personal data and defines more clearly the conditions of data processing in light of the new technological advances and the principle of accountability.

IV INTERNATIONAL DATA TRANSFER AND DATA LOCALISATION

Regarding international transfers, Decree 1377 of 2012 differentiated between ‘transfers’ and ‘transmissions’ of personal data. Pursuant to Decree 1377, ‘data transfers’ take place when the data is shared with a controller, while ‘transmissions’ occur when the data is shared with a processor.

i International data transfers
According to Law 1581,\(^9\) international data transfers of personal data to countries that ‘do not provide an adequate level of protection for personal data’ is prohibited, unless:

\(a\) there is express consent from the data subject;

\(b\) the processing is done with the purpose of preserving the data subject’s health and life (medical data);

\(c\) they are banking or stock exchange transfers;

\(d\) they are transfers agreed in international treaties;

\(e\) they are transfers for pre-contractual or contractual performance, as long as the data subject has consented;

\(f\) transfers legally required in order to safeguard public interest or for the acknowledgment or defence in a judicial process;

Recently, the Colombian data protection authority issued a guideline that sets forth the standards that a country must comply with in order to ‘provide an adequate level of protection of personal data’, and has included a list of countries that already comply with such standards.\(^{10}\)

\(^8\) Council CONPES No. 3920 of ‘National Policy of Data Exploitation’, National Department of Planning.

\(^9\) Article 26, Law 1581 of 2012

\(^{10}\) According to Circular No. 005 of 2017, the following countries are considered to have an adequate level of protection of personal data: Germany; Australia; Austria; Belgium; Cyprus; Costa Rica; Croatia; Denmark; Slovakia; Slovenia; Estonia; Spain; the United States; Finland; France; Greece; Hungary; Ireland; Iceland;
In light of the above, transfers of data to countries included in the list published by SIC, or that provide an adequate level of protection of personal data, are permitted. Transfers sent to a country that does not provide an adequate level of protection of personal data require a declaration of conformity from SIC.

ii International data transmissions

According to Decree 1377 of 2013, international transmissions between a controller and a processor do not require express consent or to be informed to the data subject, as long as there is an agreement between the controller and the processor that determines the processing activities and the obligations of the processor in relation to the controller and the data subject. Furthermore, the contract must state that the processor shall comply with any obligation included in the controller's privacy policy and to process data according to the purposes that have been authorised by the data subjects and the law, among other related obligations.

V COMPANY POLICIES AND PRACTICES

According to the regulatory framework, organisations that process personal data are required to have a privacy policy and an internal manual of policies and proceedings.

The privacy policy must identify the controller and its contact information and include the purposes and kinds of processing that will be carried out with the data, the rights of the data subject, the person or area responsible to process claims, petitions and consultations and the proceeding to exercise the data subject's rights, among others. The privacy policy is intended to be public and to informed to all data subjects.

The internal manual of policies and procedures, on the other hand, is expected to include the internal proceedings and policies that the company has put into place in order to comply with the data protection regulation.

Furthermore, organisations are expected to comply with the principle of accountability, set forth in Decree 1377 of 2013 that establishes that controllers must be able to demonstrate that they have implemented internal policies to comply with Law 1581 that are proportional to: (1) the organisation's nature, structure and size (2) the nature of the data that is being processed (3) the kind of processing being made and (4) the potential risks that processing may cause.

The internal policies must guarantee the existence of an administrative structure proportional to the structure and size of the company, the adoption of mechanisms to implement the internal policies, including implementation tools, training and education programmes, and the adoption of proceedings to answer any queries, petitions and claims made by data subjects.

Furthermore, the Superintendence of Industry and Commerce has issued the Guideline to Implement the Principle of Accountability, which serves as reference to organisations in order to implement the principle of accountability within their organisations.

Law 1581 requires companies to register the existence of their databases in a National Registry of Databases administered by SIC. Although the obligation exists since Law 1581...
was enacted in 2012, the deadline for organisations to comply with this requirement has not yet ended. Owing to the novelty and cumbersomeness of the registration proceeding, the government has extended the term for registration several times.

VI DISCOVERY AND DISCLOSURE

Article 10 of Law 1581 establishes some processing of personal data that do not require consent of the data subject. Among them, Article 10 sets forth that controllers or processors are allowed to disclose or provide personal data to public or administrative entities that require it, as long as these entities are acting within their powers, or when the disclosure is requested by judicial order.

Discovery and disclosure of personal data to foreign administrative and judicial authorities should comply with international treaties signed by Colombia, and either be channelled through a rogatory letter or other proceedings included in the Hague Convention, of which Colombia is signatory.

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

Colombia’s data protection authority is SIC and, within it, the Deputy Superintendence of Personal Data Protection.

As the data protection authority, SIC is in charge of enforcing data protection regulation and has the power to carry out unannounced audits and raids, as well as investigate and penalise non-compliance with the law.

ii Penalties

SIC has the power to open investigations against any organisation that is considered to be infringing the data protection laws and enforce the law. According to the results of the investigation, SIC has the power to

- impose fines of up to 2,000 minimum wages;
- order the suspension of activities related to data processing for up to six months while corrections are implemented;
- order temporary closure of all operations related to processing when correctives are not implemented during the suspension; and
- order the immediate or definitive closure of operations related to sensitive data.

Since 2010, SIC has imposed more than 620 sanctions for a total of 21 million pesos.

iii Recent enforcement cases

Fine for failing to delete contact data from databases

One of the most important newspaper and media companies in Colombia was recently fined for failing to suppress the contact data from a user after the user had repeatedly asked the company to delete his data from all databases of the company. Once the company received the request, it proceeded to delete the data from two databases but the data remained in the
main database of the company, so the user continued to receive commercial information. The graduation of the penalty took into account that this was not the first time the company had been investigated for the same kind of complaint.

**Suspension of activities for six months**

The investigated company was a retail seller dedicated to telephone marketing. The company had built its databases with contact data obtained from telephone directories. In the view of the company, telephone directory data was public data and thus exempted it from acquiring consent from the data subject. SIC ruled that the telephone number of data subjects is not considered public data but as semi-private data, and, therefore the company required express consent from data subjects in order to include them in the company’s marketing database. In light of the above, SIC ordered the suspension of the company’s activities for six months while the company obtained proper consent from data subjects. The decision was appealed and the final decision is still pending.

**Private litigation**

Law 1581 does not provide for specific remedies or financial recovery for private plaintiffs. However, other actions such as class contractual or tort actions are also available to data subjects, but are still not common.

**VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS**

According to Law 1581, the Colombian Data Protection law applies to data processing that is carried out within Colombia or when according to the law or international treaties Colombian law is applicable to the controller or processor located outside Colombia.

Jurisdictional issues for multinational organisations may arise owing to the interaction between local corporate vehicles and their mother companies, which may entail a transfer or transmission of personal data.

Colombian data protection regulation requires consent for almost any kind of processing and provides few exceptions to the consent rule. Therefore, it is advisable for multinational organisations to verify that their internal corporate policies (particularly those related to transfers and transmissions in and out of the country) comply with local standards.

**IX CYBERSECURITY AND DATA BREACHES**

i **Criminal prosecution of cybersecurity and data protection infractions**

The Colombian Criminal Code punishes several crimes related to cybersecurity and data protection infractions. Among them, the Criminal Code punishes abusive access to computing systems, illegitimate blocking or hindering of computing systems or telecommunication networks, interception of computing data, computing damages, use of malicious software, illegitimate use of personal data and phishing, among others.

---

11 Article 2, Law 1581 of 2012.
Data breaches in the data protection regulation

Pursuant to Law 1581, controllers must report to the SIC any security incident that enables or threatens unauthorised access or use of personal data. Controllers must report the incident within 15 business days of learning of the incident, and include in the report the kind of incident, the date of occurrence and the date on which the organisation learned of the incident, the kind of data and number of data subjects affected, causes and potential consequences of the incident and correctives that the organisation has applied or will apply. Organisations may present the report directly to the SIC or through the National Registry of Databases platform.

OUTLOOK

Article 27 of Law 1581 established that the government must adopt a regulation regarding binding corporate rules. Although SIC has conducted a study on the matter, the government has not yet issued the regulation, but is expected to do so.

On the other hand, it is important to note that although the EU’s new General Data Protection Regulation is not applicable in Colombia, many domestic organisations are interested in complying with such regime in order to be able to offer their products or services in the EU.
Chapter 11

GERMANY

Olga Stepanova

I  OVERVIEW

Germany has been and still is the forerunner on privacy and data protection law. In 1970, the German state of Hesse enacted the world’s first Data Protection Act. The other states soon followed, and on 1 January 1978, the first German Federal Data Protection Act (BDSG) entered into force. These acts established basic principles of data protection, such as the requirement of a legal permission or the data subject’s consent for any processing of personal data. In 1983, the German Federal Constitutional Court held that the individual even has a constitutional right to ‘informational self-determination’. The background of this groundbreaking verdict was a census planned for the year 1983, which essentially focused on the census of the entire German population by the means of electronic data processing. The people of Germany were anything but pleased with this idea and – as a consequence – more than 1,600 complaints were filed at the Federal Constitutional Court against the census law that had been specifically adopted for the census by the German parliament. Finally, in December 1983, the German Federal Constitutional Court declared certain provisions of the Census Act to be unconstitutional.

Over time, the German Federal Data Protection Act was subsequently amended in order to meet the requirements of a society in which data processing grew more important. Especially, digitalisation raised a lot of questions, which needed to be handled. Keeping this in mind, among others the legislator passed the German Telemedia Act (TMA) in 2007, which stipulated the duty to safeguard data protection during the operation of telemedia services. However, since data protection law and telemedia law got increasingly intersected by the internet, it was planned by the European legislator that the ePrivacy Regulation replacing the TMA would also come into force at the same time as the General Data Protection Regulation (GDPR). The GDPR entered into force on 25 May 2018 as scheduled. The ePrivacy Regulation is still subject to tripartite negotiations and will probably be applicable in 2020. For this reason, the following text provides an overview of the current legal situation in Germany, presenting the changes and the challenges of a new era of data protection in connection with digitalisation.

II  THE YEAR IN REVIEW

The past year was marked by the upcoming adoption of Regulation (EU) 2016/679, the GDPR, which replaced the German data protection laws to a large extent.

1 Olga Stepanova is an associate at Winheller Rechtsanwaltsgesellschaft mbH.
As a regulation, the new framework does not have to be transposed into the different national laws of the European countries but is directly applicable in all EU Member States. However, as a specialty of the GDPR, the regulation also contains ‘opening clauses’ that provide Member States with the discretion to introduce additional national provisions to concretise and further specify the application of the GDPR for specific issues (e.g., in connection with employees). To that end, the German parliament passed a new version of the BDSG in April 2017. This new set of rules, the GDPR and the new German BDSG, both became effective in May 2018.

It was interesting to see how the GDPR became popular in mass media, which happens with very few laws, so even tabloid newspapers were reporting about upcoming changes every day. Due to the fact that the GDPR has always been mentioned in connection with the high penalties stipulated in Article 83 GDPR, a kind of public fear grew, which led to a high level of insecurity, even among customers who used messaging services, email services and social media.

Although the GDPR maintains the main concepts of data protection as we knew them before, or amends details of them (e.g., data processing is still prohibited if not explicitly permitted by the data subject or a law, the legal bases for the transfer of personal data into non-EU countries or the obligation to designate a data protection officer), the new rules also bring some important changes. Small companies and non-profit organisations, in particular, are unsure about how to implement the GDPR.

First and foremost, the GDPR extended its territorial scope, which means that non-European companies may also fall within its scope, making it the first worldwide data protection law due to globalisation. It applies to (1) all companies worldwide that target European markets and in this context process the personal data of European Union citizens (irrespective of where the processing takes place) and (2) those that process the data of European citizens in the context of their European establishments. The GDPR tightens the rules for obtaining valid consent to process personal information. Still, valid consent is one of the two possibilities to justify data processing, the other option is legal justification. Companies will therefore have to assess their processes to make sure they process personal data lawfully, and to review whether it is advisable to refrain from seeking consent but to switch to legal justification with fewer prerequisites and no possibility of being revoked at any time.

As a consequence, upon request of data protection authorities, companies have to provide prove that they fulfil their obligations under the GDPR. The authorities do not need to investigate and prove the infringements by themselves anymore. The GDPR also introduced mandatory privacy impact assessments (PIAs). It requires data controllers to conduct PIAs where privacy breach risks are high to minimise risks to data subjects. This means that before organisations can begin projects involving special categories of personal data, such as health, they will have to conduct a PIA and work with the data protection offices to ensure they are in compliance with data protection laws as projects progress.

Additionally, the GDPR expanded liability beyond the data controllers. In the past, only data controllers were considered responsible for data processing activities, but the GDPR extended liability to all organisations that process personal data. The GDPR also covers any organisation that provides data processing services to the data controller, which means that even organisations that are purely service providers that work with personal data will need to comply with rules such as data minimisation.
The enforcement of the GDPR is backed by significant fines of up to €20 million or 4 per cent of annual global turnover, whichever is higher.

To sum it up, the increase of obligations and fines are also likely to force previously idle organisations to rethink their positions.

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

The GDPR defines personal data as 'any information relating to an identified or identifiable natural person'. This definition applies to all personal data handled by electronic information and communication (telemedia) service providers.

However, all of these data are now subject to the GDPR, as the German Data Protection Conference presented a paper on 26 April 2018, which states that Article 95 GDPR has to be interpreted in a way that the provisions of TMA governing the data protection shall not be applicable anymore. Following this opinion, there is no privileged handling for data collection via telemedia anymore, so the controllers must obey the strict rules prescribed by the GDPR from now on.

ii General obligations for data handlers

The privacy provisions of the GDPR address data controllers, namely entities that process personal data on their own behalf or commission others to do the same. Telemedia service providers as data collectors may collect and use personal data only to the extent that the law specifically permits, or if the data subject has given his or her consent, Article 6 GDPR. Moreover, to the extent that the law permits the collection of data for specified purposes, these data may not be used for other purposes, unless the data subject has consented to other uses.

According to Articles 13 and 14 GDPR, the controller must, inter alia, inform the user of the extent and purpose of the processing of personal data for any consent to be valid. Consent may be given electronically, provided the data controller ensures that the user of the service declares his or her consent knowingly and unambiguously, the consent is recorded, the user may view his or her consent declaration at any time and the user may revoke consent at any time with effect for the future. These principles accord with Article 7 GDPR, which requires consent to be based on the voluntary and informed decision of the data subject. Consent, however, is not always required. Former, many statutory exceptions allow for the use of data without consent, for various business-related purposes. Though, following the aforementioned paper, controllers cannot make use of them since 25 May 2018. Therefore, controllers are now forced to find new ways to guarantee lawful processing while collecting data through websites, apps and by electronic communication. This also goes along with a proper assessment of previous data-processing procedures and can lead to increased shifts of service providers that are not able or not willing to comply with the high standards of GDPR.

iii Technological innovation and privacy law

Cookies

Under data protection law, the use of cookies is only relevant if the information stored in the cookie is considered personal data. A cookie is a piece of text stored on a user’s computer by his or her web browser. It may be used for authentication, storing site preferences, the identifier
for a server-based session, shopping cart contents or anything else that may be accomplished through the storage of text data. The cookie is considered to be personal data if it contains data that allow the controller to identify the data subject. However, before the GDPR entered into force, and as long as the relevant part of TMA was still applicable, cookies could have been placed in Germany as long as the user had the option to object (opt out). Now, there is no such privileged treatment anymore as the general requirements regarding a lawful data processing are applicable for cookies too. The only question not answered so far by the European Court of Justice (ECJ) is whether the use of cookies must inevitably be based on the data subject’s consent (Article 6(1)(a) GDPR) or is it sufficient when the controller states that this use is necessary for the purposes of his legitimate interest (Article 6(1)(f) GDPR). In any case, according to the German Data Protection Conference, prior consent is required for the use of tracking mechanisms, which pursue the behaviour of affected persons on the internet and create user profiles. That means, that informed consent within the meaning of the GDPR is required in the form of a declaration or other clearly confirmatory action taken prior to data processing (i.e., before cookies are placed on the user’s device).2

The reason for this discussion and the legal uncertainty is derived from the fact that the ePrivacy Regulation did not enter into force on time and has not even been passed. So far, it may be advisable to fulfil the requirements of the GDPR in its whole scope, which means that consent has to be sought before tracking the user.

Social media

Social media becomes more popular each day as the number of users grows. The same applies to the opportunities and smart solutions offered by using these media. Most social media platforms are free of charge. Users pay with their personal data, even though many of them are not even aware of this fact. That is why the European legislator stipulated in the principles of processing in Article 5 GDPR inter alia that processing has to be transparent and the processor shall be responsible for obeying this principle. Therefore, one can find a lot of other regulations realising the legislator’s will by creating a sharp sword against Big Data companies, which are often suspected of processing data in an unlawful way.

The first decision against Facebook was ruled by the ECJ just 11 days after the GDPR became effective (ECJ, 5 June 2018 – C-210/16). Admittedly, the original case dates back seven years. At that time, the German Schleswig-Holstein State Centre for Data Protection had asked the Academy of Economics to delete its fansite on Facebook and issue a ban order. The background to this was the fact that neither Facebook nor the Business Academy informed visitors about the data they had collected. After several instances, the case finally ended up before the German Federal Administrative Court, which referred the question of the responsibility for the data collection of the fansite operators to the ECJ, because the fansite operator only had very limited access to the data records of the individual fansite visitors collected by Facebook.

For many, the ECJ’s relatively harsh verdict against fansite operators was surprising. Although the main responsibility for data collection lies with Facebook, it is theoretically possible for the page operators to place cookies on the visitor’s device, even if the visitor does not have a Facebook account. According to the ECJ, this in addition to the fact that

fansite operators receive the visitor’s user data (even if only anonymised) and can use these for parameterisation lead to joint responsibility of the site operators. This is particularly because of the fact that the collection of this data cannot (yet) be deactivated. Until Facebook grants this option to its users, the common fansite operator remains jointly responsible for the collection of user data. Even the ECJ takes account of the significant imbalance in the use of data between Facebook and the operators of the respective fan page insofar as the degree of responsibility can be assessed differently in individual cases, however, in the court’s opinion Facebook and the fansite operators are still joint controllers. In the end, Facebook will have to react to implementing mechanisms like cookie banners or others to give the user access to information. However, this decision and the German Federal Court’s decision regarding the obligation of Facebook to provide heirs with access to the digital postbox of the decedent (BGH, 12 July 2018 – III ZR 183/17), clearly show that social media is now being regulated more strictly.

IV INTERNATIONAL DATA TRANSFER AND DATA LOCALISATION

The international transfer of personal data is regulated within the framework of Articles 44–50 GDPR. There is a general distinction between transfers within the EU and EEA or to one of the ‘trusted countries’ for which the European Commission has confirmed by means of an ‘appropriateness decision’ that these countries ensure an adequate level of data protection on the one hand and transfers to third countries on the other. For an international data transfer to be lawful, it must comply not only with the aforementioned articles, but must also be in compliance with the general provisions pertaining to the legality of processing operations involving personal data.

i Data transfer within the EU or EEA

In contrast to the former legal situation, the GDPR does not explicitly stipulate that there is no difference between transfers within Germany or within EU or EEA. Therefore, the only distinction is made between domestic transfers (within the EU or EEA) and those outside the EU or EEA.

ii Data transfer to countries outside the EU or EEA

If a private entity intends to transfer personal data internationally to another entity located outside the area of the EU or EEA (a third country), Article 44 GDPR specifies the requirements for such a transfer. In this respect, personal data shall not be transferred when the data subject has a legitimate interest in being excluded from the transfer. A legitimate interest is assumed when an adequate level of data protection cannot be guaranteed in the country to which the data are transferred.

An adequate level of data protection exists in certain third countries that have been identified by the European Commission. These are Andorra, Argentina, Guernsey, the Isle of Man, Canada (limited), the Faroe Islands, Israel (limited), Guernsey, Jersey, New Zealand, Switzerland and Uruguay. Any transfer of personal data to these countries will only have to satisfy the requirements of domestic data transfers.

Uncertainty currently surrounds data transfers to the United States. After the European Court of Justice declared the Safe Harbour principles of the Commission invalid, the Commission enacted the EU–US Privacy Shield. Under the protection of the new principles
of the Privacy Shield the United States is found to have an adequate level of data protection. But the Privacy Shield itself is again the target of a great deal of criticism. There are currently several complaints pending against the Privacy Shield at the European Court of Justice.

Data transfers to any other non-EU country may be justified by the derogation rules of Article 49 GDPR. Accordingly, the international transfer of personal data is admissible if:

1. the data subject has given his or her consent;
2. the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject’s request;
3. the transfer is necessary for the conclusion or performance of a contract that has been or is to be concluded in the interest of the data subject between the controller and a third party;
4. the transfer is necessary for Important reasons of public interest;
5. the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims;
6. the transfer is necessary to protect the vital interests of the data subject; or
7. the transfer is made from a register that is intended to provide information to the public, and that is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down in law are fulfilled in the particular case.

The most relevant grounds are those given in (b), namely if the transfer is necessary to perform a contract between the data subject and the controller. This includes international monetary transactions and distance-selling contracts as well as employment contracts. All transfers in this respect have to be essential for the purposes of the contract.

Any consent within the meaning of (a) will only be valid if the data subject was informed about the risks that are involved in data transfers to countries that do not have an adequate standard of data protection. In addition, the consent has to be based on the data subject’s free will; this may be difficult if employee data are involved.

If none of the aforementioned exceptions applies, the transfer of personal data to third countries with an inadequate level of data protection is nonetheless possible if, among other requirements, the competent supervisory authority authorises the transfer. Such an authorisation will only be granted when the companies involved adduce adequate safeguarding measures to compensate for a generally inadequate standard of data protection, see Article 49(1)2 GDPR. However, the primary safeguarding measures are the use of standard contractual clauses issued by the European Commission and the establishment of binding corporate rules.

V PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

Germany has a Federal Data Protection Agency and 16 state data protection agencies. These often act in concert when making recommendations on how customers can navigate safely through the internet. In addition, German experts often discuss the data protection problems that arise from the widespread collection of data by search engines and social media, and the use of these data to profile the data subject for commercial purposes.
The state data protection agencies are charged with supervising the data privacy compliance of state entities, as well as all non-public entities whose principal place of business is established in the state and that are not subject to the exclusive jurisdiction of the federal supervisory authority. In states that have enacted a freedom of information act, the state supervisory authorities are typically also charged with supervising the act’s application by state entities.

The heads of the supervisory authorities are typically appointed by the federal and state parliaments respectively, and are required to report to their respective parliaments.

ii  **Material enforcement cases**

One of the most discussed amendments specified by the GDPR and the new BDSG is the dramatic increase of the framework for fines. Before, the fines for data protection breaches were up to €300,000 per breach. Now, fines are up to €20 million or, in the case of an undertaking, up to 4 per cent of the total worldwide annual turnover of the preceding financial year, whichever is higher. This massive increase is directly addressed to Big Data companies. Especially the dynamic and the dependency on the turnover aims to achieve a deterrent effect even on the most be wealthiest companies worldwide. However, no fine has been imposed so far, thus everyone highly awaits the supervising authorities’ first fines to estimate the further development and risks. However, the reasons for data protection breaches have not changed. Mostly they are caused by internal compliance activities of companies where the responsible management carelessly contravened the high standards of data protection law (e.g., through video surveillance or keylogging). Another source of data protection breaches is the lack of employee training, which shall ensure that everybody in the company has the necessary knowledge to handle personal data in a lawful way.

iii  **Private litigation**

The GDPR imposes duties of notification on the data controller (see Articles 13 and 14 GDPR). He or she must notify the data subject among others, the identity and the contact details of the controller, the contact details of the data protection officer, if applicable, the purposes of the processing and the legal basis, the source of the data, where applicable, to whom they are disclosed, the duration of processing and the retention policy, etc. Additionally, the data subject has to be informed regarding all his or her rights granted by the GDPR. In detail, this notification has to contain information concerning the right to information, right to rectification, right to be forgotten, right to restriction of processing, right to data portability, right to object and the right to lodge a complaint with a supervisory authority. This enumeration clearly shows that on the one hand the data subject is getting a lot of rights, on the other hands the controller will have invest more effort to satisfy the requests in a proper way, which is a question of time and expenses. The privacy rights and remedies of telemedia users are governed to a large extent by Article 77 GDPR (the right to lodge a complaint with a supervisory authority) and Article 82 GDPR (the right to compensation). Data subjects may enforce their rights through the judicial remedies provided in civil law. Injunctive relief as well as damages can be claimed. Especially, damages for pain and suffering from data protection violations can be claimed under civil law.

In Germany, the data protection authorities are not necessarily involved in enforcing the rights of individual data subjects. Instead, complaints against domestic controllers must first be lodged with the company’s in-house data protection officer.
However, in the event of unsatisfactory contact with the company data protection officer, the supervisory authority and the civil courts can of course be called in.

VI CONSIDERATIONS FOR FOREIGN ORGANISATIONS

As data protection gradually becomes a questions of technical measures, especially cybersecurity, Article 32 GDPR determines that pseudonymisation and encryption has to be applied to lower the risk of damaging the data subject in case of data breaches.

The implementation of such and similar technical measures may safeguard the controller from notifying a data breach to the relevant authority as the risk to the rights and freedoms of natural persons had been reduced from the start. These measures became even more important with GDPR, as one can easily notice that the legal situation demands a higher ability to act. As Article 33(1) GDPR stipulates that data breaches, where feasible, shall be notified by the controller to the supervising authority within 72 hours. Therefore, controllers have to implement an effective data protection management system to be able to meet the deadline. Otherwise, a violation of this provision alone can be punished with a fine of up to €10 million or in the case of an undertaking, up to 2 per cent of the total worldwide annual turnover of the preceding financial year.

VII OUTLOOK

The GDPR is still an unknown and often only can be understood by a teleological interpretation. In Germany, there are 16 data protection authorities that follow different interpretations of the GDPR text. This complicates advising in privacy matters. Therefore, it will be interesting to see how the new laws will be interpreted by German and European courts. Furthermore, we are looking forward to seeing what impact the GDPR will have on companies, especially social media operators.
Chapter 12

HONG KONG

Yuet Ming Tham

I OVERVIEW

The Personal Data (Privacy) Ordinance (PDPO) establishes Hong Kong’s data protection and privacy legal framework. All organisations that collect, hold, process or use personal data (data users) must comply with the PDPO, and in particular the six data protection principles (DPPs) in Schedule 1 of the PDPO, which are the foundation upon which the PDPO is based. The Office of the Privacy Commissioner for Personal Data (PCPD), an independent statutory body, was established to oversee the enforcement of the PDPO.

Hong Kong was the first Asian jurisdiction to enact comprehensive personal data privacy legislation and to establish an independent privacy regulator. Unlike the law in several other jurisdictions in the region, the law in Hong Kong covers both the private and public sectors. Hong Kong issued significant new amendments to the PDPO in 2012 with a key focus on direct marketing regulation and enforcement with respect to the use of personal data.

Despite Hong Kong’s pioneering role in data privacy legislation, the PCPD’s level of activity with respect to regulatory guidance and enforcement has been relatively flat in the past year. In addition, Hong Kong has not introduced stand-alone cybercrime or cybersecurity legislation as other Asian countries have done. Certain sectoral agencies, notably Hong Kong’s Securities and Futures Commission (SFC), have continued to press forward on cybersecurity regulation for specific industries.

This chapter discusses recent data privacy and cybersecurity developments in Hong Kong from August 2017 to July 2018. It will also discuss the current data privacy regulatory framework in Hong Kong, and in particular the six DPPs and their implications for organisations, as well as specific data privacy issues such as direct marketing, issues relating to technological innovation, international data transfer, cybersecurity and data breaches.

II THE YEAR IN REVIEW

i Personal data privacy and security developments

From mid-2015 to mid-2016, the PCPD issued a number of guidance notes, guidelines and codes of practice to assist organisations in implementing PDPO provisions. Notable publications included the October 2015 Guidance on Data Breach Handling and the Giving of Breach Notifications, the April 2016 Revised Code of Practice on Human Resource
Management, the April 2016 Privacy Guidelines: Monitoring and Personal Data Privacy at Work and the June 2016 guidance note on Proper Handling of Data Access Request and Charging of Data Access Request Fee by Data Users. None of these publications are legally binding, although failure to follow the codes of practice may give rise to negative presumptions in any enforcement proceedings.

From mid-2016 to mid-2017, the PCPD did not issue any additional codes of practice or guidelines, but did release three revisions to existing guidance notes:

- **Guidance on Data Breach Handling and the Giving of Breach Notifications (revised December 2016)** (providing assistance to data users in handling breaches and mitigating loss and damage);
- **Guidance on CCTV Surveillance and Use of Drones (revised March 2017)** (setting out recommendations on whether and how to use CCTV to properly protect data privacy); and
- **Proper Handling of Data Correction Request by Data Users (revised May 2017)** (providing a step-by-step approach on the proper handling of a data correction request under the PDPO).

From mid-2017 to mid-2018, the PCPD issued a new guidance note in December 2017 entitled Guidance on Election Activities for Candidates, Government Departments, Public Opinion Research Organisations and Members of the Public. Additionally, the PCPD released revised Guidance on CCTV Surveillance and Use of Drones.

The PCPD reported that it had received 3,501 complaints in 2017, which included 1,968 complaints relating to the reported loss of laptops by the Registration and Electoral Office containing personal data of election committee members and electors (the REO Incident). Excluding those complaints, the remaining 1,533 complaints represents a 17 per cent decrease from the 1,838 complaints received in 2016. Most of the complaints involved were made against private sector organisations, with financial, property management, and telecommunications companies leading the way. Forty-one per cent of the complaints related to use of personal data without consent with about one-third complaining about the purpose and manner of the data collection. The PCPD received 237 ICT-related privacy complaints in 2017, representing a 3 per cent increase as compared to 2016. Most of these complaints related to the use of mobile apps and social networking websites. The PCPD received notice of 106 data breach incidents affecting 3.87 million persons in 2017 compared to 89 incidents involving 104,000 individuals the year before; however, taking out the REO Incident

---

(which affected 3.78 million people), the number of affected individuals was only 86,000, representing a decrease of 17 per cent as compared to 2016. Direct marketing complaints decreased substantially in 2017, falling from 393 to 186 cases.

With respect to enforcement in 2017, the PCPD issued 26 warnings and three enforcement notices as compared to 36 warnings and six enforcement notices in 2016. Referrals to the police of cases for criminal prosecutions fell substantially compared to 2016, from 112 to 19, almost all of which involved direct marketing violations. The number of actual prosecutions remained relatively flat (four prosecutions in 2017 compared to five in 2016). All four prosecutions in 2017 resulted in convictions. One was for a company director who failed to comply with a summons issued by the Privacy Commissioner, and the other three concerned direct marketing violations. In January 2018, PARKnSHOP pled guilty to using the personal data of a data subject in direct marketing without obtaining the data subject’s consent, resulting in a HK$3,000 fine.\(^\text{12}\)

The PCPD does not systematically publish decisions or reports based on the outcome of its investigations. For the entirety of 2017 and up until June 2018, the PCPD published one investigation report\(^\text{13}\) in 2017 (offering recommendations to estate agencies in ensuring compliance with the requirements under the PDPO).

**ii  Cybercrime and cybersecurity developments**

Hong Kong does not have (and as of this writing, there do not appear to be plans to establish) stand-alone cybercrime and cybersecurity legislation. The Hong Kong Police Department maintains a resource page for ‘Cybersecurity and Technology Crime’, including a compendium of relevant legislation on computer crimes.\(^\text{14}\) These specific provisions relate to the Crimes Ordinance, the Telecommunications Ordinance and laws related to obscenity and child pornography. The government has also established an Information Security (InfoSec) website that sets out various computer crime provisions contained in the Telecommunications Ordinance, the Theft Ordinance and the Crimes Ordinance.\(^\text{15}\) According to the Hong Kong police, there were 5,939 computer crime cases in 2016, with an associated loss of HK$2.3 billion as compared to 6,862 cases in 2015 amounting to a loss of HK$1.8 billion.\(^\text{16}\) (Figures were not available for 2017 as of the time of writing.)

Sectoral regulators have continued to press forward with specific cybersecurity regulation, particularly financial regulators. Both the SFC and the Hong Kong Monetary Authority (HKMA) have issued circulars on cybersecurity risk, and in May 2017, the SFC issued its Consultation Paper on Proposals to Reduce and Mitigate Hacking Risks Associated with Internet Trading,\(^\text{17}\) as well as a circular alert on ransomware threats in the securities sector.

---


industry. In December 2016, the HKMA announced implementation details of its Cybersecurity Fortification Initiative undertaken in collaboration with the banking industry as well as launching an industry-wide Enhanced Competency Framework on Cybersecurity.

iii 2018 developments and regulatory compliance

From a regulatory perspective, the key compliance framework for companies and organisations remains with data protection and privacy. The government has not taken any additional legislative steps in the cybercrime and cybersecurity arenas although cybersecurity remains a significant challenge in Hong Kong. Financial sector regulators continue to be active with respect to cybersecurity, with the HKMA putting forward ambitious initiatives. For companies outside the financial sector, their focus will remain with PDPO compliance, particularly with the stringent direct marketing requirements.

III REGULATORY FRAMEWORK

i The PDPO and the six DPPs

The PDPO entered into force on 20 December 1996 and was amended by the Personal Data (Privacy) (Amendment) Ordinance 2012 (Amendment Ordinance). The majority of the provisions of the Amendment Ordinance entered into force on 1 October 2012 and the provisions relating to direct marketing and legal assistance entered into force on 1 April 2013.

The PCPD has issued various codes of practice and guidelines to provide organisations with practical guidance to comply with the provisions of the PDPO. Although the codes of practice and guidelines are only issued as examples of best practice and organisations are not obliged to follow them, in deciding whether an organisation is in breach of the PDPO, the PCPD will take into account various factors, including whether the organisation has complied with the codes of practice and guidelines published by the PCPD. In particular, failure to abide by certain mandatory provisions of the codes of practice will weigh unfavourably against the organisation concerned in any case that comes before the Privacy Commissioner. In addition, a court is entitled to take that fact into account when deciding whether there has been a contravention of the PDPO.

As mentioned above, the six DPPs of the PDPO set out the basic requirements with which data users must comply in the handling of personal data. Most of the enforcement notices served by the PCPD relate to contraventions of the six DPPs. Although a contravention of the DPPs does not constitute an offence, the PCPD may serve an enforcement notice on data users for contravention of the DPPs, and a data user who contravenes an enforcement notice commits an offence.

DPP1 – purpose and manner of collection of personal data

Principle

DPP1 provides that personal data shall only be collected if it is necessary for a lawful purpose directly related to the function or activity of the data user. Further, the data collected must be adequate but not excessive in relation to that purpose.

---

Data users are required to take all practicable steps to ensure that on or before the collection of the data subjects’ personal data (or on or before first use of the data in respect of item (d) below), the data subjects were informed of the following matters:

\[ a \] the purpose of collection;
\[ b \] the classes of transferees of the data;
\[ c \] whether it is obligatory to provide the data, and if so, the consequences of failing to supply the data; and
\[ d \] the right to request access to and request the correction of the data, and the contact details of the individual who is to handle such requests.

Implications for organisations

A personal information collection statement (PICS) (or its equivalent) is a statement given by a data user for the purpose of complying with the above notification requirements. It is crucial that organisations provide a PICS to their customers before collecting their personal data. On 29 July 2013, the PCPD published the Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement, which serves as guidance for data users when preparing their PICS. It is recommended that the statement in the PICS explaining what the purpose of the collection is should not be too vague and too wide in scope, and the language and presentation of the PICS should be user-friendly. Further, if there is more than one form for collection of personal data each serving a different purpose, the PICS used for each form should be tailored to the particular purpose.

DPP2 – accuracy and duration of retention

Principle

Under DPP2, data users must ensure that the personal data they hold are accurate and up to date, and are not kept longer than necessary for the fulfilment of the purpose.

After the Amendment Ordinance came into force, it is provided under DPP2 that if a data user engages a data processor, whether within or outside Hong Kong, the data user must adopt contractual or other means to prevent any personal data transferred to the data processor from being kept longer than necessary for processing the data. ‘Data processor’ is defined to mean a person who processes personal data on behalf of a data user and does not process the data for its own purposes.

It should be noted that under Section 26 of the PDPO, a data user must take all practicable steps to erase personal data held when the data are no longer required for the purpose for which they were used, unless any such erasure is prohibited under any law or it is in the public interest not to have the data erased. Contravention of this Section is an offence, and offenders are liable for a fine.

Implications for organisations

The PCPD published the Guidance on Personal Data Erasure and Anonymisation (revised in April 2014), which provides advice on when personal data should be erased, as well as how personal data may be permanently erased by means of digital deletion and physical destruction. For example, it is recommended that dedicated software, such as that conforming to industry standards (e.g., US Department of Defense deletion standards), be used to permanently delete data on various types of storage devices. Organisations are also advised to adopt a top-down approach in respect of data destruction, and this requires the development
of organisation-wide policies, guidelines and procedures. Apart from data destruction, the guidance note also provides that the data can be anonymised to the extent that it is no longer practicable to identify an individual directly or indirectly. In such cases, the data would no longer be considered as ‘personal data’ under the PDPO. Nevertheless, it is recommended that data users must still conduct a regular review to confirm whether the anonymised data can be re-identified and to take appropriate action to protect the personal data.

**DPP3 – use of personal data**

**Principle**

DPP3 provides that personal data shall not, without the prescribed consent of the data subject, be used for a new purpose. ‘Prescribed consent’ means express consent given voluntarily and that has not been withdrawn by notice in writing.

**Implications for organisations**

Organisations should only use, process or transfer their customers’ personal data in accordance with the purpose and scope set out in their PICS. If the proposed use is likely to fall outside the customers’ reasonable expectation, organisations should obtain express consent from their customers before using their personal data for a new purpose.

**DPP4 – data security requirements**

**Principle**

DPP4 provides that data users must use all practicable steps to ensure that personal data held are protected against unauthorised or accidental processing, erasure, loss or use.

After the Amendment Ordinance came into force, it is provided under DPP4 that if a data user engages a data processor (such as a third-party IT provider to process personal data of employees or customers), whether within or outside Hong Kong, the data users must adopt contractual or other protections to ensure the security of the data. This is important, because under Section 65(2) of the PDPO, the data user is liable for any act done or practice engaged in by its data processor.

**Implications for organisations**

In view of the increased use of third-party data centres and the growth of IT outsourcing, the PCPD issued an information leaflet entitled ‘Outsourcing the Processing of Personal Data to Data Processors’, in September 2012. According to this leaflet, it is recommended that data users incorporate contractual clauses in their service contracts with data processors to impose obligations on them to protect the personal data transferred to them. Other protection measures include selecting reputable data processors, and conducting audits or inspections of the data processors.

The PCPD also issued the Guidance on the Use of Portable Storage Devices (revised in July 2014), which helps organisations to manage the security risks associated with the use of portable storage devices. Portable storage devices include USB flash cards, tablets or notebook computers, mobile phones, smartphones, portable hard drives and DVDs. Given that large amounts of personal data can be quickly and easily copied to such devices, privacy could easily be compromised if the use of these devices is not supported by adequate data protection policies and practice. The guidance note recommended that a risk assessment be carried out to guide the development of an organisation-wide policy to manage the risk.
associated with the use of portable storage devices. Further, given the rapid development of technology, it is recommended that this policy be updated and audited regularly. Some technical controls recommended by the guidance note include encryption of the personal data stored on the personal storage devices, and adopting systems that detect and block the saving of sensitive information to external storage devices.

**DPP5 – privacy policies**

*Principle*

DPP5 provides that data users must publicly disclose the kind of personal data held by them, the main purposes for holding the data, and their policies and practices on how they handle the data.

*Implications for organisations*

A privacy policy statement (PPS) (or its equivalent) is a general statement about a data user’s privacy policies for the purpose of complying with DPP5. Although the PDPO is silent on the format and presentation of a PPS, it is good practice for organisations to have a written policy to effectively communicate their data management policy and practice. The PCPD published a guidance note entitled Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement, which serves as guidance for data users when preparing their PPS. In particular, it is recommended that the PPS should be in a user-friendly language and presentation. Further, if the PPS is complex and lengthy, the data user may consider using proper headings and adopting a layered approach in presentation.

**DPP6 – data access and correction**

*Principle*

Under DPP6, a data subject is entitled to ascertain whether a data user holds any of his or her personal data, and to request a copy of the personal data. The data subject is also entitled to request the correction of his or her personal data if the data is inaccurate.

Data users are required to respond to a data access or correction request within a statutory period of 40 days. If the data user does not hold the requested data, it must still inform the requestor that it does not hold the data within 40 days.

*Implications for organisations*

Given that a substantial number of disputes under the PDPO relate to data access requests, the PCPD published a guidance note entitled Proper Handling of Data Access Request and Charging of Data Access Request Fee by Data Users, dated June 2012, to address the relevant issues relating to requests for data access. For example, although a data user may impose a fee for complying with a data access request, a data user is only allowed to charge the requestor for the costs that are ‘directly related to and necessary for’ complying with a data access request. It is recommended that a data user should provide a written explanation of the calculation of the fee to the requestor if the fee is substantial. Further, a data user should not charge a data subject for its costs in seeking legal advice in relation to the compliance with the data access request.
ii Direct marketing

Hong Kong’s regulation of direct marketing deserves special attention from organisations engaging in such activities. Unlike with violations of the DPPs, violations of the PDPO’s direct marketing provisions are criminal offences, punishable by fines and by imprisonment. The PCPD has demonstrated a willingness to bring enforcement actions in this area and to refer particularly egregious violations for criminal prosecution.

Revised direct marketing provisions under the PDPO

The revised direct marketing provisions under the Amendment Ordinance entered into effect on 1 April 2013, and introduced a stricter regime that regulates the collection and use of personal data for sale and for direct marketing purposes.

Under the revised direct marketing provisions, data users must obtain the data subjects’ express consent before they use or transfer the data subjects’ personal data for direct marketing purposes. Organisations must provide a response channel (e.g., email, online facility or a specific address to collect written responses) to the data subject through which the data subjects may communicate their consent to the intended use. Transfer of personal data to another party (including the organisation’s subsidiaries or affiliates) for direct marketing purposes, whether for gain or not, will require express written consent from the data subjects.

Guidance on Direct Marketing

The PCPD published the New Guidance on Direct Marketing in January 2013 to assist businesses to comply with the requirements of the revised direct marketing provisions of the PDPO.

Direct marketing to corporations

Under the New Guidance on Direct Marketing, the Privacy Commissioner stated that in clear-cut cases where the personal data are collected from individuals in their business or employee capacities, and the product or service is clearly meant for the exclusive use of the corporation, the Commissioner will take the view that it would not be appropriate to enforce the direct marketing provisions.

The Privacy Commissioner will consider the following factors in determining whether the direct marketing provisions will be enforced:

a the circumstances under which the personal data are collected: for example, whether the personal data concerned are collected in the individual’s business or personal capacity;

b the nature of the products or services: namely, whether they are for use of the corporation or for personal use; and

c whether the marketing effort is targeted at the business or the individual.

Amount of personal data collected

While the Privacy Commissioner has expressed that the name and contact information of a customer should be sufficient for the purpose of direct marketing, it is provided in the New Guidance on Direct Marketing that additional personal data may be collected for direct marketing purposes (e.g., customer profiling and segmentation) if the customer elects to supply the data on a voluntary basis. Accordingly, if an organisation intends to collect additional personal data from its customers for direct marketing purposes, it must inform
its customers that the supply of any other personal data to allow it to carry out specific purposes, such as customer profiling and segmentation, is entirely voluntary, and obtain written consent from its customers for such use.

**Penalties for non-compliance**

Non-compliance with the direct marketing provisions of the PDPO is an offence, and the highest penalties are a fine of HK$1 million and imprisonment for five years.

**Spam messages**

Direct marketing activities in the form of electronic communications (other than person-to-person telemarketing calls) are regulated by the Unsolicited Electronic Messages Ordinance (UEMO). Under the UEMO, businesses must not send commercial electronic messages to any telephone or fax number registered in the do-not-call registers. This includes text messages sent via SMS, pre-recorded phone messages, faxes and emails. Contravention of the UEMO may result in fines ranging from HK$100,000 to HK$1 million and up to five years’ imprisonment.

In early 2014, the Office of the Communications Authority prosecuted a travel agency for sending commercial facsimile messages to telephone numbers registered in the do-not-call registers. This is the first prosecution since the UEMO came into force in 2007. The case was heard before a magistrate’s court, but the defendant was not convicted because of a lack of evidence.

**Person-to-person telemarketing calls**

Although the Privacy Commissioner has previously proposed to set up a territory-wide do-not-call register on person-to-person telemarketing calls, this has not been pursued by the government in the recent amendment of the PDPO. Nevertheless, under the new direct marketing provisions of the PDPO, organisations must ensure that they do not use the personal data of customers or potential customers to make telemarketing calls without their consent. Organisations should also check that the names of the customers who have opted out from the telemarketing calls are not retained in their call lists.

On 5 August 2014, the Privacy Commissioner issued a media brief to urge the government administration to amend the UEMO to expand the do-not-call registers to include person-to-person calls. In support of the amendment, the Privacy Commissioner conducted a public opinion survey, which revealed that there had been a growing incidence of person-to-person calls, with more people responding negatively to the calls and fewer people reporting any gains from the calls. Although there had been long-standing discussions regarding the regulation of person-to-person calls in the past, it remains to be seen whether any changes will be made to the legislation.

**Enforcement**

Following prosecution referrals by the PCPD, Hong Kong courts handed down the first penalties in direct marketing violations in 2015. In September 2015, the Hong Kong Magistrates’ Court convicted the Hong Kong Broadband Network Limited (HKBN) for violating the PDPO’s requirement that a data user cease using an individual’s personal data in

---

direct marketing upon request by that individual.\textsuperscript{22} The court imposed a fine of HK$30,000. In a separate court action from September 2015, Links International Relocation Limited pleaded guilty to a PDPO direct marketing violation for not providing required information to a consumer before using his personal data in direct marketing.\textsuperscript{23} The court fined the company HK$10,000.

Additional convictions and fines followed in 2015 and 2016 for direct marketing violations. The most recent cases initiated by the PCPD resulting in fines and convictions were a January 2017 guilty plea by DBS Bank for failing to comply with a customer request to cease using personal data in direct marketing, resulting in a HK$10,000 fine,\textsuperscript{24} and a December 2016 guilty plea from a watch company that failed to obtain consent and to inform the consumer of his rights under the PDPO before engaging in direct marketing to the consumer, resulting in a HK$16,000 fine.\textsuperscript{25} Given the large number of criminal referrals by the PCPD with respect to direct marketing violations, we expect direct marketing prosecutions to continue to be an active enforcement area.

\textbf{iii \hspace{1em} Technological innovation and privacy law}

\textit{Cookies, online tracking and behavioural advertising}

While there are no specific requirements in Hong Kong regarding the use of cookies, online tracking or behavioural advertising, organisations that deploy online tracking that involves the collection of personal data of website users must observe the requirements under the PDPO, including the six DPPs.

The PCPD published an information leaflet entitled ‘Online Behavioural Tracking’ (revised in April 2014), which provides the recommended practice for organisations that deploy online tracking on their websites. In particular, organisations are recommended to inform users what types of information are being tracked by them, whether any third party is tracking their behavioural information and to offer users a way to opt out of the tracking.

In cases where cookies are used to collect behavioural information, it is recommended that organisations preset a reasonable expiry date for the cookies, encrypt the contents of the cookies whenever appropriate, and do not deploy techniques that ignore browser settings on cookies unless they can offer an option to website users to disable or reject the cookies.

The PCPD also published the Guidance for Data Users on the Collection and Use of Personal Data through the Internet (revised in April 2014), which advises organisations on compliance with the PDPO while engaging in the collection, display or transmission of personal data through the internet.

\textit{Cloud computing}

The PCPD published the information leaflet ‘Cloud Computing’ in November 2012, which provides advice to organisations on the factors they should consider before engaging in cloud computing. For example, organisations should consider whether the cloud provider

\textsuperscript{22} www.pcpd.org.hk/english/news_events/media_statements/press_20150909.html. HKBN appealed, and in 2017, the Hong Kong High Court dismissed the appeal, confirming that HKBN’s communication was for the purpose of direct marketing. See www.onc.hk/en_US/can-data-user-received-data-subjects-opt-request-continue-promote-services-part-sale-service.


\textsuperscript{24} www.pcpd.org.hk/english/news_events/media_statements/press_20170110.html.

has subcontracting arrangements with other contractors, and what measures are in place to ensure compliance with the PDPO by these subcontractors and their employees. In addition, when dealing with cloud providers that offer only standard services and contracts, the data user must evaluate whether the services and contracts meet all security and personal data privacy protection standards they require.

On 30 July 2015, the PCPD published the revised information leaflet ‘Cloud Computing’ to advise cloud users on privacy, the importance of fully assessing the benefits and risks of cloud services and the implications for safeguarding personal data privacy. The new leaflet includes advice to organisations on what types of assurances or support they should obtain from cloud service providers to protect the personal data entrusted to them.

**Employee monitoring**

In April 2016, the PCPD published the revised Privacy Guidelines: Monitoring and Personal Data Privacy at Work, to aid employers in understanding steps they can take to assess the appropriateness of employee monitoring for their business, and how they can develop privacy-compliant practices in the management of personal data obtained from employee monitoring. The guidelines are applicable to employee monitoring activities whereby personal data of employees are collected in recorded form using the following means: telephone, email, internet and video.

Employers must ensure that they do not contravene the DPPs of the PDPO while monitoring employees’ activities. The PDPO has provided some additional guidelines on monitoring employees’ activities and has recommended employers to do the following:

a) Evaluate the need for employee monitoring and its impact upon personal data privacy. Employers are recommended to undertake a systematic three-step assessment process:

- ‘assessment’ of the risks that employee monitoring is intended to manage and weigh that against the benefits to be gained;
- ‘alternatives’ to employee monitoring and other options available to the employer that may be equally cost-effective and practical but less intrusive on an employee’s privacy; and
- ‘accountability’ of the employer who is monitoring employees, and whether the employer is accountable and liable for failure to be compliant with the PDPO in the monitoring and collection of personal data of employees.

b) Monitor personal data obtained from employee monitoring. In designing monitoring policies and data management procedures, employers are recommended to adopt a three-step systematic process:

- ‘clarify’ in the development and implementation of employee monitoring policies the purposes of the employee monitoring; the circumstances in which the employee monitoring may take place; and the purpose for which the personal data obtained from monitoring records may be used;
- ‘communication’ with employees to disclose to them the nature of, and reasons for, the employee monitoring prior to implementing the employee monitoring; and
- ‘control’ over the retention, processing and the use of employee monitoring data to protect the employees’ personal data.
IV INTERNATIONAL DATA TRANSFER AND DATA LOCALISATION

Section 33 of the PDPO deals with the transfer of data outside Hong Kong, and it prohibits all transfers of personal data to a place outside Hong Kong except in specified circumstances, such as where the data protection laws of the foreign country are similar to the PDPO or the data subject has consented to the transfer in writing. Section 33 of the PDPO has not been brought into force since its enactment in 1995, and although implementation has been consistently discussed in recent years, the government currently has no timetable for its implementation.

V COMPANY POLICIES AND PRACTICES

Organisations that handle personal data are required to provide their PPS to the public in an easily accessible manner. In addition, prior to collecting personal data from individuals, organisations must provide a PICS setting out, inter alia, the purpose of collecting the personal data and the classes of transferees of the data. As mentioned above, the PCPD has published the Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement (see Section III.i), which provides guidance for organisations when preparing their PPS and PICS.

The Privacy Management Programme: A Best Practice Guide (see Section II.i) also provides guidance for organisations to develop their own privacy policies and practices. In particular, it is recommended that organisations should appoint a data protection officer to oversee the organisation's compliance with the PDPO. In terms of company policies, apart from the PPS and PICS, the Best Practice Guide recommends that organisations develop key policies on the following areas: accuracy and retention of personal data; security of personal data; and access to and correction of personal data.

The Best Practice Guide also emphasises the importance of ongoing oversight and review of the organisation's privacy policies and practices to ensure they remain effective and up to date.

VI DISCOVERY AND DISCLOSURE

i Discovery

The use of personal data in connection with any legal proceedings in Hong Kong is exempted from the requirements of DPP3, which requires organisations to obtain prescribed consent from individuals before using their personal data for a new purpose (see Section III.i). Accordingly, the parties in legal proceedings are not required to obtain consent from the individuals concerned before disclosing documents containing their personal data for discovery purposes during legal proceedings.

ii Disclosure

Regulatory bodies in Hong Kong, such as the Hong Kong Police Force, the Independent Commission Against Corruption and the Securities and Futures Commission, are obliged to comply with the requirements of the PDPO during their investigations. For example, regulatory bodies in Hong Kong are required to provide a PICS to the individuals prior to collecting information or documents containing their personal data during investigations.
Nevertheless, in certain circumstances, organisations and regulatory bodies are not required to comply with DPP3 to obtain prescribed consent from the individuals concerned. This includes cases where the personal data are to be used for the prevention or detection of crime, and the apprehension, prosecution or detention of offenders, and where compliance with DPP3 would be likely to prejudice the aforesaid purposes.

Another exemption from DPP3 is where the personal data is required by or authorised under any enactment, rule of law or court order in Hong Kong. For example, the Securities and Futures Commission may issue a notice to an organisation under the Securities and Futures Ordinance requesting the organisation to produce certain documents that contain its customers’ personal data. In such a case, the disclosure of the personal data by the organisation would be exempted from DPP3 because it is authorised under the Securities and Futures Ordinance.

VII PUBLIC AND PRIVATE ENFORCEMENT

i Public enforcement
An individual may make a complaint to the PCPD about an act or practice of a data user relating to his or her personal data. If the PCPD has reasonable grounds to believe that a data user may have breached the PDPO, the PCPD must investigate the relevant data user. As mentioned above, although a contravention of the DPPs does not constitute an offence in itself, the PCPD may serve an enforcement notice on data users for contravention of the DPPs, and a data user who contravenes an enforcement notice commits an offence.

Prior to the amendment of the PDPO in 2012, the PCPD was only empowered to issue an enforcement notice where, following an investigation, it is of the opinion that a data user is contravening or is likely to continue contravening the PDPO. Accordingly, in previous cases where the contraventions had ceased and the data users had given the PCPD written undertakings to remedy the contravention and to ensure that the contravention would not continue or recur, the PCPD could not serve an enforcement notice on them as continued or repeated contraventions were unlikely.

Since the entry into force of the Amendment Ordinance, the PCPD has been empowered to issue an enforcement notice where a data user is contravening, or has contravened, the PDPO, regardless of whether the contravention has ceased or is likely to be repeated. The enforcement notice served by the PCPD may direct the data user to remedy and prevent any recurrence of the contraventions. A data user who contravenes an enforcement notice commits an offence and is liable on first conviction for a fine of up to HK$50,000 and two years’ imprisonment and, in the case of a continuing offence, a penalty of HK$1,000 for each day on which the offence continues. On second or subsequent conviction, the data user would be liable for a fine of up to HK$100,000 and imprisonment for two years, with a daily penalty of HK$2,000.

ii Private enforcement
Section 66 of the PDPO provides for civil compensation. Individuals who suffer loss as a result of a data user’s use of their personal data in contravention of the PDPO are entitled to compensation by that data user. It is a defence for data users to show that they took reasonable steps to avoid such a breach.

After the Amendment Ordinance came into force, affected individuals seeking compensation under Section 66 of the PDPO may apply to the Privacy Commissioner for
assistance and the Privacy Commissioner has discretion whether to approve it. Assistance by the Privacy Commissioner may include giving advice, arranging assistance by a qualified lawyer, arranging legal representation or other forms of assistance that the Privacy Commissioner may consider appropriate.

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

Although the PDPO does not confer extraterritorial application, it applies to foreign organisations to the extent that the foreign organisations have offices or operations in Hong Kong. For example, if a foreign company has a subsidiary in Hong Kong, the Hong Kong subsidiary will be responsible for the personal data that it controls, and it must ensure the personal data are handled in accordance with the PDPO no matter whether the data are transferred back to the foreign parent company for processing.

IX CYBERSECURITY AND DATA BREACHES

1 Cybercrime and cybersecurity

As previously noted, Hong Kong does not have stand-alone cybercrime or cybersecurity legislation. The Computer Crimes Ordinance, which was enacted nearly 25 years ago in 1993, amended the Telecommunications Ordinance,26 the Crimes Ordinance27 and the Theft Ordinance,28 expanding the scope of existing criminal offences to include computer-related criminal offences. These include:

a unauthorised access to any computer; damage or misuse of property (computer program or data);
b making false entries in banks’ books of accounts by electronic means;
c obtaining access to a computer with the intent to commit an offence or with dishonest intent; and
d unlawfully altering, adding or erasing the function or records of a computer.

Although Hong Kong does not currently have cybersecurity legislation, the government does support a number of organisations dedicated to responding to cyber threats and incidents. These entities include the Hong Kong Emergency Response Team Coordination Centre (managed by the Hong Kong Productivity Council) for coordinating responses for local enterprises and internet users, and the Government Computer Emergency Response Team Hong Kong (a work unit established under the Office of the Government Chief Information Officer), which is a team charged with coordinating and handling incidents relating to both the private and public sectors. In addition, the Hong Kong Police Force has established the Cyber Security and Technology Crime Bureau, which is responsible for handling cybersecurity issues and combating computer crime.

---

26 Sections 24 and 27 of the Telecommunications Ordinance.
27 Sections 59, 60, 85 and 161 of the Crimes Ordinance.
28 Sections 11 and 19 of the Theft Ordinance.
Data breaches

There is currently no mandatory data breach notification requirement in Hong Kong. In October 2015 and then again in December 2016, the PCPD revised its Guidance on Data Breach Handling and the Giving of Breach Notifications, which provides data users with practical steps in handling data breaches and to mitigate the loss and damage caused to the individuals involved. Although the PCPD noted in the Guidance that there are no statutory notification requirements, the PCPD recommended that data users strongly consider notifying affected persons and relevant authorities, such as the PCPD. In particular, after assessing the situation and the impact of the data breach, the data users should consider whether the following persons should be notified as soon as practicable:

a. the affected data subjects;
b. the law enforcement agencies;
c. the Privacy Commissioner (a data breach notification form is available on the PCPD’s website);
d. any relevant regulators; or
e. other parties who may be able to take remedial actions to protect the personal data privacy and the interests of the data subjects affected (e.g., internet companies such as Google and Yahoo! may assist in removing the relevant cached link from their search engines).

OUTLOOK

Hong Kong’s data privacy and protection framework is long-standing and relatively mature. We expect that the PCPD will continue enforcement at generally the same levels, with continued emphasis on direct marketing violations and prosecution referrals for such violations.

In recent public statements, the PCPD has emphasised the importance of striking a balance between privacy protection and free flow of information, engaging small- and medium-sized businesses in promoting the protection of and respect for personal privacy, and strengthening the PCPD’s working relationship with mainland China and overseas data protection authorities. We expect that the PCPD and the Hong Kong government will continue to emphasise the development of Hong Kong as Asia’s premier data hub and to provide additional policy, promotional and incentive support to facilitate growth in the region.

With respect to cybercrime and cybersecurity, we do not anticipate major legislation in the near term and expect that sectoral regulators will continue to take the lead in these areas.
Chapter 13

HUNGARY

Tamás Gödölle

I OVERVIEW

The new constitution of Hungary (the Fundamental Law) was adopted in 2011 and entered into force on 1 January 2012. The Fundamental Law contains a section on ‘Freedom and Responsibility’, which describes the fundamental rights of individuals. Article VI(1) of the Fundamental Law generally provides that everyone is entitled to respect for his or her private and family life, home, communications and good reputation, whereas Article VI(2) provides for the right to the protection of personal data as well as for the right to access and disseminate information of public interest. In addition, Article VI(3) states that an independent authority shall be responsible for the enforcement of the protection of personal data and freedom of access to data of public interest.

The Hungarian Civil Code, which was adopted in 2013 and entered into force on 15 March 2014, also contains provisions concerning privacy rights. The general rules on the protection of personality rights (including the right for the protection of personal data) are set out in the Civil Code, which provides the basic rules for civil law relationships. Accordingly, personality rights can be exercised freely within the framework of the law and within the rights of others. The exercise of such rights shall not be impeded by any other person. However, personality rights shall not be considered as having been violated if the person has given prior consent.

Although the above legislation contains general principles and clauses, the recent introduction of the European General Data Protection Regulation (GDPR) has caused quite a change in Hungary’s single legislative privacy regime. The general rules of the protection of personal data and freedom of information from 25 May 2018 are contained in the GDPR and Act CXII of 2011 on Informational Self-Determination and Freedom of Information (the Privacy Act) will be secondary to the general rules that are to be applied throughout the European Union. As of July 2018, the bill for the amendment of the Privacy Act, for the sake of GDPR compliance, is being discussed by the Hungarian parliament. It is likely that the final version of the Privacy Act will be published later in the summer. It is interesting that a draft for the amendment had been issued for comments by professionals last autumn, but it was withdrawn because the government was not satisfied with the draft, and now the same amendment is being discussed by the parliament even though it suffers from the same defects as last autumn, namely that the draft did not make use of the possible points of departure from the GDPR text where it is allowed.

1 Tamás Gödölle is a partner at Bogsch & Partners Law Firm.
2 The translation of the consolidated version of the Fundamental Law of Hungary is available at www.kormany.hu/download/e/02/00000/The%20New%20Fundamental%20Law%20of%20Hungary.pdf.
In the meantime the Privacy Act underwent a minor modification so that the Hungarian Data Protection Authority (DPA) has been appointed to act as a supervisory authority under the GDPR. This minor amendment also stipulated that the legal consequences of a breach of data protection laws will be punished with just a warning for the first time if this is possible under the circumstances of the case.

The entity responsible for enforcing the data protection law is the DPA. The DPA aims to guarantee the rights of individuals to exercise control over their privacy and to have access to data of public interest and public data on the grounds of public interest. The GDPR and the Privacy Act are regarded as background legislation for specific statutes regulating the collection and processing of personal data.

The GDPR and the Privacy Act should be considered as the general legislation providing rules regarding the protection of personal data and the disclosure of public data. Beyond this scope, there are other sectoral acts (e.g., the Labour Code, Electronic Communications Act, etc.) that provide additional data protection-related provisions. The processing of medical, criminal, electoral and citizenship data is regulated by other acts.

In Hungarian data privacy regulation, the role of NGOs and self-regulatory industry groups, as well as society or advocacy groups, is marginal, and there are no specific Hungarian laws providing for government surveillance powers.

The government approved the National Cybersecurity Strategy, which determines the national objectives and strategic directions, tasks and comprehensive government tools to enable Hungary to enforce its national interests in Hungarian cyberspace, within the context of the global cyberspace. The strategy aims to develop a free and secure cyberspace and to protect national sovereignty.

II THE YEAR IN REVIEW

The year 2018 so far has been all about the preparation for the new regime of the GDPR. Many related publications and opinions have been issued by private sector market participants and also by the DPA, however, it can be stated that the DPA follows the general guidelines of the Working Party 29 in all matters, therefore most of the DPA’s guidelines can be considered as translations of the guidelines used throughout the EU.

As a first-wave preparation aid, the DPA published a localised version3 of the UK Information Commissioner’s Office’s 12-point list on how to get ready for the GDPR. Subsequently, in its annual report,4 the DPA dedicated a whole chapter to analysing and describing the most important developments of the GDPR, and even provided comparisons with the local Privacy Act to explain the key changes that the GDPR will introduce when it enters into force.

As mentioned earlier, at the end of August 2017, a bill of law has been submitted to the parliament with the aim of harmonising the Privacy Act with the new – directly applicable – GDPR. The general and detailed debate on the bill, and hopefully its adoption, will take place in the summer session as discussed above.

In 2018 the DPA has seen its staff expanded and approximately 40 colleagues have been hired to ensure that the DPA is able to handle the workload caused by the changes resulting from the introduction of the GDPR.

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

The GDPR and the Privacy Act regulate the protection of personal data in Hungary. The GDPR, in force since 25 May 2018, and the Act, which was enacted in 2011 and entered into force on 1 January 2012,5 purports to guarantee the right of everyone to exercise control over his or her personal data and to have access to data of public interest.

There are two categories of protected information: 'personal data' and 'sensitive data'. There is also a third category of data named 'data of public interest'; this is beyond the scope of the GDPR but the Privacy Act contains regulations for this category of data, as well.

Personal data

The GDPR and the Privacy Act apply to all data processing and technical data processing that is carried out in Hungary or that aims at Hungarian data subjects, and that pertains to the data of physical persons. The GDPR and the Privacy Act regulate the processing of data carried out wholly or partially by automatic means, and the manual processing of data.

Personal data are defined in Article 3.2 of the Act as any data relating to the data subject – a specific (directly or indirectly identified or identifiable) natural person – and any conclusion with respect to the data subject that can be inferred from that data, in particular by reference to his or her name, identification code or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity. For the purposes of the GDPR, the term personal data is very similar: '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.

Sensitive data

The term ‘special data’ (sensitive data) is defined by the Privacy Act as information on a data subject’s racial and national origin, political opinion or party affiliation, religious or ideological beliefs, or membership of any special interest organisations, as well as his or her state of health, pathological addictions, sex life or criminal personal data.6 Now the GDPR provides a similar term as follows: processing 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 shall be prohibited.

Please note that the basic standpoint of the GDPR is different from the approach of the Privacy Act, as the GDPR prescribes that the processing of categories of sensitive data is prohibited and they may be processed only if certain exceptions listed in GDPR Article 9(2) are applicable.

---


6 Ibid., Article 3(3).
The Privacy Act also protects data of public interest and data that are public on grounds of public interest. The term ‘data of public interest’ is defined to include any information or knowledge, not falling under the definition of personal data, processed by an organ or person performing a state or local government function or other public function determined by law.7

**Data controller**

A data controller has been defined by the Privacy Act as any natural or legal person, or any organisation without legal personality, who or which, alone or jointly with others, determines the purpose of the processing of personal data, makes decisions on data processing (including those as to the means of the processing), and implements these decisions or has them implemented by the technical data processor he or she has assigned, whereas the new GDPR contains the following definition: ‘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.

**Data processor**

The Act identifies a ‘data processor’ as any natural or legal person or organisation without legal personality that carries out the technical processing of personal data based on a contract with the data controller – including the conclusion of a contract pursuant to a rule of law. Under the GDPR ‘processor’ means a natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller.

The GDPR and the Act apply to both types of data processing entities, namely data controllers and data processors, with some different provisions applying to technical data processing.

The data controller is always responsible for the lawfulness of the instructions given for the data processing operations of its outsourced data processor.

The data processor shall process personal data in compliance with the specific instructions of the data controller; consequently, the processor cannot make any decisions concerning data processing.

It has been noted that, as of 1 July 2013, a data processor may contract out processing operations to another processor in line with the instructions of the data controller.8 This regulation is also incorporated into the GDPR by default.

**Data protection audits**

With effect from 1 January 2013, the DPA provides data protection audits as a service to data controllers who request it. The DPA may charge an administrative fee for the audit that cannot exceed 5 million forints. The relevant aspects of DPA audits have been published on the DPA’s website.9 This will be possible even in the GDPR era but there will be other means as well to check the data protection law compliance: prior consultation in accordance with Article 36 GDPR as a data controller shall consult the supervisory authority (i.e., the

---

7 ibid., Article 3(5).
8 ibid., Article 10(2), as amended, effective as of 1 July 2013.
Hungary

DPA) prior to processing where a data protection impact assessment under Article 35 GDPR indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

Protection of consumers

The Direct Marketing Act identifies numerous obligations for marketing organisations to ensure the protection of consumers, and particularly restricts the use of the name and home address of natural persons for marketing purposes.\(^\text{10}\) Notably, the provisions of the Direct Marketing Act are only applicable where the marketing materials are sent by post. Marketing materials sent by electronic means are regulated by the Advertising Act and the e-Commerce Act. In this regard the GDPR brings some novelties as Recital (47) contains that the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest and this implies that no consent is required as a legal basis for such data processing which means a significant change from the previous Hungarian approach. It is also true that the above indicated Hungarian Acts are in conflict with the GDPR as they have not been amended yet, therefore the Hungarian situation may be regarded as dubious as long as the domestic laws are not made to be compliant with the GDPR.

ii General obligations for data handlers

According to the GDPR Processing shall be lawful only if and to the extent that at least one of the following applies:

\(a\) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

\(b\) 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;

\(c\) processing is necessary for compliance with a legal obligation to which the controller is subject;

\(d\) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

\(e\) 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; and

\(f\) 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 that require protection of personal data, in particular where the data subject is a child.

Before collecting information from an individual, the controller must indicate to the data subject whether data processing is based on consent or relies on any other legal ground. In addition, the data controller must provide the data subject with unambiguous and detailed information on all the facts relating to the processing of his or her data in line with Article 13/14 GDPR.

Regarding online data, Act CVIII of 2001 on Certain Issues of Electronic Commerce Services and Information Society Services provides, *inter alia*, that information means any

\(^{10}\) Direct Marketing Act, Section 5.
data, signal or image that can be processed, stored and transmitted by electronic means irrespective of whether its content is protected by law; and information society service means remote services provided by electronic means, generally for payment, and accessed by the recipient of the service individually.

According to this Act, the service provider may process personal data that is suitable and sufficient for the identification of the recipient of the service for the purposes of:

- drawing up a contract for the service in question;
- determining and modifying the contents and monitoring the performance of the service;
- charging for the service; and
- enforcing claims relating to the service.

The recipient of the service shall be allowed – at all times before and during the course of using the information society service – to prohibit the data processing.

Requirements of preliminary notices

As mentioned above, data controllers must provide data subjects with unambiguous and adequately detailed information on the circumstances of the processing of his or her personal data. On 9 October 2015, the DPA issued an official recommendation regarding the minimum requirements for preliminary notices provided to data subjects prior to the commencement of the processing of their personal data. While these recommendations are generally considered soft law, in the event of an investigation, the DPA will check whether the data controller meets these requirements. This recommendation continues to be in force as it is compliant with the GDPR text.

The recommendation sets out general principles regarding the quality and accessibility of notices, and also contains explanations pertaining to the applicable provisions of the Privacy Act. According to the recommendation, preliminary notices shall:

- be clear: repeating the words of the Privacy Act is not adequate, and the use of everyday wording is suggested;
- be readable and comprehensible: the text of the notice shall be structured and easy to understand;
- align with the set of concerned data subjects: if during the course of the data processing the set of data subjects can be easily determined, then the notice shall align with the specific requirements of the data subjects;
- not be considered a legal statement: the notice itself is not a legal statement. However, the information therein may have a greater impact on the data subjects’ consent (which is a legal statement). Should the notice be considered a legal statement, its clarity and transparency would be weakened by the details required by law;
- describe unique data processing: the document fulfils its role as a notice if it contains the unique data processing regulations concerning the specific data controller; and
- be available and accessible: the notice shall always be accessible for the data subject at the time when his or her personal data are being collected.

For the purposes of preliminary notices Articles 13 and 14 of the GDPR shall also be taken into consideration.

**Data security incident register**\(^\text{12}\)

According to Article 15(1a) of the Privacy Act, for subsequent countermeasure examinations by the DPA and for data subject notification purposes, the data controller shall keep a record of all data regarding data security incidents. The register shall contain:

- the personal data concerned;
- the scope and number of subjects affected by the data security incident;
- the date, time, circumstances and effects of the incident; and
- countermeasures carried out.

Additionally, GDPR introduced a new regime for notifying data breaches to the DPA and in certain cases to the data subjects. The detailed rules can be found in Articles 33 and 34 GDPR: 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 supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. The notification shall contain the nature of the personal data breach, name and contact details of the data protection officer, the likely consequences and the measures taken or proposed to be taken by the controller to address the personal data breach.

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.

**Database registration requirements**

Under the new GDPR rules, the DPA does not keep a registry of data processing activities.

**Rights of data subjects**

Articles 15-21 GDPR contain the rights of the data subjects, such as: right of access by the data subject, rectification and erasure (right to be forgotten), restriction of processing, right to data portability and the right to object. Data subjects may request information on the processing of their personal data, such as which data are processed by the data controller or its data processors; about the purpose of the processing, its legal basis, its duration and the name, address and activity of the data processor; and, should there be one, on the circumstances of any data protection incident.\(^\text{13}\) They also have the right to know who has received or will receive their data, and for what purpose. The data controller must give this information within a month and in an easily understandable manner. Data controllers must provide this information in written form if this is requested by the data subject.

The GDPR and the Privacy Act requires data controllers to rectify any inaccurate personal data. In addition, it provides for the deletion of personal data if the processing is unlawful, if this has been requested by the data subject, or if this has been ordered by a court

---

\(^\text{12}\) Implemented in 2015. Applicable from 1 October 2015.

\(^\text{13}\) Implemented in 2015. Applicable from 1 October 2015.
or the DPA. 14 A data controller must delete data that is incomplete or inaccurate and cannot be corrected in a lawful way, unless the deletion is prohibited by another law. It must also destroy data when the purpose of processing has ceased to exist, or when the time limit for the storage of the data has expired.

**Right to objection**

Article 21 of the Privacy Act and Article 21 of the GDPR grant data subjects the right to object to the processing of their data in numerous circumstances. These include, for example, when the processing is necessary only for enforcing a right or legitimate interest of the data controller or third party, unless the data processing has been ordered by law.

When an objection has been filed, the data controller must suspend the use of the data while investigating the complaint. It must respond to the request promptly, within a month.

**Redress and enforcement rights**

Any individual may file a complaint with the DPA if he or she thinks that his or her rights have been violated, or that there is an imminent danger of such a violation, except when judicial proceedings are already pending concerning the case in question.

Under the GDPR the maximum sum of a data protection fine that can be imposed upon a person or entity responsible for a data security incident increased to 10 or 20 million Euros, respectively, for different breaches of data protection law as detailed in Article 83(4)–(5) GDPR.

Data controllers are held liable under the Privacy Act and the GDPR for any damage suffered by data subjects as a result of the unlawful processing of their data or the infringement of the data protection requirements in the Privacy Act. As of 15 March 2014, the data subject may also claim exemplary damages – namely, lump sum damages that can be awarded by the court as compensation for harm sustained from the infringement of privacy rights by the data controller as a result of unlawful data processing or a breach of data security requirements.

### iii Technological innovation and privacy law

More detailed regulatory frameworks apply to several data privacy issues.

**Employee monitoring**

The Labour Code generally authorises employers to introduce monitoring measures. 15 It allows employers to monitor the conduct of employees; however, such measures may be taken only in the context of employment. Further, the means used for monitoring may not violate the human dignity of the worker. To exclude all possibility of doubt, the Labour Code also states that the private life of the employee cannot be monitored, which is in conformity with the practice of the European Court of Human Rights. In addition, the employer must give notice to employees, in advance, of the use of technical means serving to control or monitor employees’ conduct.

---

14 Data Protection Law, Article 17(2).
15 Labour Code, Article 11.
On 30 January 2013, the DPA issued a recommendation on video surveillance in the workplace, which addresses the issues of legal basis, guarantees, data retention, notice and registration requirements relating to the operation of surveillance systems.\(^ {16}\)

Based upon the DPA's recommendation, if video surveillance involves or affects third parties (such as visitors), the DPA must be notified of the data processing relating to the surveillance system. Notification and registration are also required if the surveillance system is not operated by the employer directly, but by a service provider (security service) that is considered the sole controller of the system.

On 28 October 2016, the DPA issued a guideline concerning the basic requirements for workplace data processing operations.\(^ {17}\) The guideline consists of two major parts, the general principles and the special rules for specific data processing operations.

In the first chapter, the guideline compares the principles (purpose, limitation, necessity and proportionality) of the Privacy Act and the Labour Code, and concludes with a joint interpretation of them with respect to workplace data processing activities. Certain privacy-related legal constructs are also explained from a labour law point of view, such as the legal basis of the data processing (consent, mandatory processing, and legitimate interest), the requirement to provide privacy notices to the data subjects prior to the commencement of processing, and cross-border transmission of employee personal data.

The second chapter of the guideline contains basic requirements concerning data processing operations for the following purposes:

- a) job applications (including anonymous job applications);
- b) monitoring applicants’ social media history;
- c) retention of applications and CVs;
- d) data processing by private employment agencies;
- e) aptitude tests;
- f) ability to require a clean criminal record from employees;
- g) workplace CCTV surveillance;
- h) monitoring the use of corporate email accounts;
- i) monitoring the use of corporate portable devices (laptops and notebooks);
- j) monitoring internet usage on corporate devices;
- k) monitoring the use of corporate mobile phones;
- l) applicability of use and implementation of GPS navigation systems;
- m) applicability of use and implementation of biometric systems; and
- n) requirements for the operation and maintenance of whistle-blowing systems.

**Restriction on cookies**

In November 2009, the European Commission adopted Directive 2009/136/EC (2009 Directive), and this amendment was to be implemented in the laws of each of the European Union Member States by 25 May 2011.

Article 3(5) of the 2009 Directive was implemented in Hungary by Section 155(4) of the Hungarian Act on Electronic Communications, which generally provides that data may

\(^{16}\) The guidance is available in Hungarian at: http://naih.hu/files/Ajanlas-a-munkahelyi-kameras-megfigyelésről.pdf.

\(^{17}\) The guideline is available in Hungarian at: http://naih.hu/files/2016_11_15_Tajekoztato_munkahelyi_adatkezelesek.pdf.
be stored or accessed on the terminal equipment of the subject end user or subscriber after
the provision of clear and comprehensive information, including the purpose of the data
processing, if the corresponding consent of the end user or subscriber has been granted.

Cloud Computing Circular released by the HFSA
The Hungarian Financial Supervisory Authority (HFSA) – which merged with the Central
Bank of Hungary on 1 October 2013 – released an executive circular (4/2012) on the
risks of public and community cloud services used by financial institutions, namely banks,
insurance companies and financial service providers in Hungary. The executive circular
qualifies the use of cloud services by financial institutions as ‘outsourcing’, and notes that
sectoral legislative rules shall be considered. Accordingly, the cloud service provider shall
comply with the same requirements applicable to financial institutions in terms of personnel,
material and security conditions.

The HFSA advises financial institutions to take into account, in a proportionate
manner, the risks of outsourcing, and to choose a provider and the technical means of
outsourcing accordingly. The HFSA announced that it would examine the legal compliance
of the technical and contractual implementation of the use of cloud services in on-site audits.

Location tracking in relation to employment
According to the most recent information from the DPA, data collected through GPS or
GSM base stations is only lawful if any device used to collect location data has a function
allowing the employee to turn the device off outside business hours. Employers may then
be able to justify their collection of the location data during business hours as continuous
monitoring is considered to be unlawful.

Automated profiling, facial recognition technology and big data
Although the EU Article 29 Working Party has published opinions on automated profiling,
facial recognition technology and big data, the DPA has not yet published any guidelines on
these matters.

iv Specific regulatory areas
The protection of children
The Privacy Act provides that children over 16 are able to give consent without additional
parental approval. Obviously, this facilitates the processing of data relating to younger people.
This is in line with the GDPR rules (Article 8 GDPR).

Health
The processing of health data is governed by the provisions of the Act on Medical Care (Act
CLIV of 1997) as well as by the Act on Handling and Protecting Medical Data (Act XLVII
of 1997). The processing of human genetic data (and research) is governed by the Act on the
Protection of Human Genetic Data and the Regulation of Human Genetic Studies, Research
and Biobanks.

The Act on Handling and Protecting Medical Data uses a very broad definition of ‘health data’. In the Act, health data are defined as:

a  any data relating to the data subject’s physical, emotional or mental status, pathological addiction, as well as the circumstances associated with disease, death or cause of death that is communicated by the data subject or by any third person in relation to the data subject, or experienced, examined, measured, extracted by or relating to the medical health service; and

b  any data in connection with or affecting the health service (including, for instance, any conduct, environment or profession). Since health data are covered by the definition of ‘special data’ under the Privacy Act, the processing of such personal information is only permitted with the written informed consent of the data subject or if explicitly ordered by the act of legislation.

The Act on Handling and Protecting Medical Data identifies the legal purposes for which health data may be processed.

For any other purposes not covered explicitly by the provisions of the Act, health data and the related personal identification data may only be processed if the patient, or his or her legal or duly authorised representative, granted his or her informed, written consent to the processing.

The Act determines the scope of persons who may lawfully process health data. The Act also regulates the strict secrecy obligations of medical personnel providing medical treatment. Medical institutions must store health records for 30 years and must store final reports for 50 years, after which time the documentation must be destroyed.

Patients have the right to be informed about the handling of their health data. They also have the right to access their health data.

**Electronic communications**

Under the provisions of the Electronic Communications Act of 2003, service providers are generally authorised to process the personal data of end users and subscribers, always to the extent required and necessary:

a  for their identification for the purpose of drawing up contracts for electronic communication services (including amendments to such contracts);

b  to monitor performance;

c  for billing charges and fees; and

d  for enforcing any related claims.

Further, the Act provides that the provision of electronic communications services may not be made dependent upon the user’s consent for processing his or her personal data; the Act on Electronic Communications defines other purposes for processing personal data.  

**Commercial communications**

Several laws address the protection of personal data in the context of commercial communications. These laws include Act CVIII of 2001 on Electronic Commerce and on

---

19  Act on Electronic Communications, Article 154(6).
Information Society Services (the e-Commerce Act), the 1995 Law on the Use of Name and Address Information Serving the Purposes of Research and Direct Marketing (the Direct Marketing Act), as well as the 2008 Act on the Basic Requirements and Certain Restrictions of Commercial Advertising Activity (the Advertising Act).

In 2001, Hungary enacted the e-Commerce Act, which requires that each commercial email clearly and unambiguously indicates that a commercial message is an electronic advertisement, and that it provides the identity of the electronic advertiser or that of the actual sender.21

The Advertising Act provides that unsolicited marketing material may not be sent to an individual without having obtained the prior, express, specific, voluntary and informed consent of the individual in compliance with the applicable provisions of the Privacy Act.22 The message must contain the email address and other contact details where the individual may request the prohibition of the transmission of electronic advertisements.23 This approach now may be changed by the above cited Recital (47) of the GDPR, however, as of now the situation is rather uncertain in Hungary, especially in absence of the new e-Privacy Regulation of the EU that will clarify the rules for direct marketing and consent. The advertiser, advertisement service provider and publisher of electronic advertisements are required to keep a register of persons who have given their consent to receiving advertisements.24 The information about these individuals may be disclosed to any third party solely upon the prior consent of the individual. Advertisers may send advertisements through email or equivalent means (e.g., text messages) to those who are listed in the register.

The Direct Marketing Act significantly restricts the use of the name and home address of natural persons for marketing purposes.25 Only a limited number of means may be used to obtain the contact details of natural persons for establishing contact (permission email). These sources include business contacts as well as phone books or statistical name listings, provided that the data subjects were informed at the time of the data gathering, and advised regarding the possibility that the data might be used for purposes other than originally intended, and of their right to prohibit such use.26

IV INTERNATIONAL DATA TRANSFER

The Privacy Act defines the term ‘transfer’ as making data accessible to a specific third party, namely, where data are passed on, whereas in the sense of the GDPR any transfer of personal data that are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if the conditions laid down in the GDPR are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. The Privacy Act defines a ‘third party’ as any

20 The e-Commerce Act is available in Hungarian at http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a0100108.tv.
21 e-Commerce Act, Article 14/A.
22 ibid., Article 14(2).
23 ibid., Article 14(3).
24 ibid., Article 14(5).
25 Direct Marketing Act, Section 5.
26 ibid., Section 3(1)(b).
natural or legal person or organisation without legal personality, other than the data subject, the data controller or the technical data processor. It follows therefore that the transfer does not include data transfers between the data subject, the data controller or the data processor.

Data transfers within the Member States of the EEA are treated as a domestic data transfer, while according to the GDPR data transfers are only such transfer that aim at transferees located in non-EEA countries.

The Privacy Act permits the transfer of personal data to a data controller or to a data processor processing personal data in a third country:

- if the data subject explicitly consents to such a transfer;
- in the event of emergency situations or in the vital interest of the data subject or a third person; or
- for the execution of an international agreement on mutual legal assistance if an adequate level of protection of personal data is ensured.

The adequate level of protection can be ensured:

- by a binding legal act of the European Union;
- by an international agreement between the third country and Hungary containing guarantees for the rights of data subjects and for the independent supervision of data control and data processing operations; and
- if the data controlling and data processing procedures comply with binding corporate rules.27

The GDPR has restructured the requirements concerning data transfers. According to the GDPR data transfers to third countries are allowed in the following cases:

- Transfers on the basis of an adequacy decision: This is the case where the European 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.
- Transfers subject to appropriate safeguards: This option incorporates especially binding corporate rules, standard data protection clauses adopted by the Commission or by the DPA (SCCs) or an approved code of conduct.
- There are also derogations for specific situations when none of the above circumstances are given. Such exceptions include when the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers or when the transfer is necessary for the performance of a contract between the data subject and the controller or when the transfer is necessary for the establishment, exercise or defence of legal claims.

For future data transfers the rules of the GDPR are applicable, while the rules of the Privacy Act will remain in force for a rather narrow scope of data processing activities where the GDPR is not applicable.

---

27 Implemented in 2015. Applicable from 1 October 2015.
V COMPANY POLICIES AND PRACTICES

There are no official codes of practice regarding company policies and practices. However, preparing internal privacy policies under Hungarian law is mandatory in some cases, such as for financial institutions, public utility companies or electronic communications service providers, which are all required to introduce internal data protection guidelines, setting out the relevant company’s compliance programme in accordance with the provisions of the Act. Nevertheless, it is also common that companies that do not fall under such an obligation – especially multinational companies who process cross-border data flows both within and outside their company group – still introduce internal privacy policies and publish privacy notices. In any case, policies containing information relating to the processing of personal data shall comply – beyond the applicable regulations of the Privacy Act – with the requirements determined by the DPA in its official recommendation of 6 October 2015 regarding privacy notices.


Under the section ‘Protection of Personal Rights’, Article 9 of the Labour Code generally articulates that everyone shall respect the personal rights of persons covered by the Act. Employers must provide notice to their employees on the processing of their personal data. Employers may only disclose facts, data and opinions concerning an employee to third persons in those cases specified by law or with the employee’s consent.

The Labour Code generally authorises employers to introduce monitoring measures. The Code provides that an employer may monitor the conduct of employees; however, such measures may be taken only in the context of employment, and the means used for monitoring may not violate the human dignity of the worker. In addition, the employer must give notice to the employee in advance of the use of technical means to control or monitor the employee’s conduct. As regards a worker’s consultation and information, the Labour Code provides that employers must consult with works councils before implementing measures and internal regulations affecting large numbers of employees. That information obligation covers, inter alia, the processing and protection of personal data of employees as well as the use of technical measures used for employee monitoring.

Restricting employee personal rights, however, is legitimate only if it matches the requirements of necessity and proportionality, namely if the restriction is definitely necessary because of a reason arising from the employment relationship and if the restriction is also proportionate for achieving its objective.

i Whistle-blowing system

Regarding the processing of employee data in whistle-blowing systems, Act CLXV of 2013 on Complaints and Public Interest Disclosure lays down the relevant rules.

The Act authorises employers to establish a system to investigate whistle-blowing reports. Conduct that may be reported includes the violation of laws as well as codes of conduct issued by the employer, provided that these rules protect the public interest or significant private interests.

The employer must publicly disclose on its corporate website the rules of conduct the violation of which may be subject to reporting, and a detailed description of the reporting procedure in Hungarian.

The investigation of a report is mandatory for employers, and the reporting person must be informed of the outcome of the investigation and of the measures taken. The identity
of the reporting person may not be disclosed without his or her consent. The Act permits the receipt and investigation of anonymous reports; however, the deadline for the investigation of such reports cannot be extended.

According to the Labour Code, employers must consult with works councils before implementing measures and internal regulations affecting large numbers of employees. This would include the implementation of a modified or new whistle-blowing system.

ii Specific provisions relating to credit data

The processing of personal data, business secrets and bank secrets by financial institutions (namely, by credit institutions and financial undertakings), data security requirements as well as data processing within the framework of the Central Credit Information System are regulated by Act CCXXXVII of 2013 on Credit Institutions and Financial Undertakings (the Banking Act).

Under the provisions of the Banking Act, credit institutions are authorised to outsource the activities connected to financial services and activities auxiliary to financial services, as well as those statutory activities prescribed by law that involve the processing of data, provided that outsourcing complies with data protection provisions. Accordingly, the outsourcing service provider must satisfy – to a degree corresponding to the risk – the personnel, infrastructure and security requirements concerning the outsourced activities that are prescribed by law for credit institutions. The Banking Act also lays down mandatory provisions for the outsourcing contract.

iii Genetic data

The processing of human genetic data is governed by Act XXI of 2008 on the Protection of Human Genetic Data and the Regulation of Human Genetic Studies, Research and Biobanks, which entered into effect on 1 July 2008. The general rules of the Act lay down that human genetic data may only be used either for the purpose of human genetic research or for medical examination. The Act guarantees the data subject’s right of information self-determination in connection with human genetic data, as it requires the written informed consent of the data subject for such data processing. Now also the GDPR deals with genetic data and provides the following definition: personal data relating to the inherited or acquired genetic characteristics of a natural person that result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained.

Genetic data is classified as a special category of personal data.

iv Data protection officer

The Privacy Act provides that selected data controllers, such as public administrative bodies, financial organisations, public utilities companies and communications companies, that customarily process huge amounts of personal data are obliged to appoint an internal data protection officer, working under the direct control and supervision of the respective data controllers’ general manager. Among the data protection officer’s various tasks, he or she is specifically responsible for:

- contributing to or assisting in decision-making related to data processing and to the enforcement of the rights of data subjects;
 monitoring compliance with the Privacy Act and other rules of law on data processing, as well as with the provisions of internal data protection and data security rules and requirements;

investigating reports submitted to him or her; and

providing the data controller or technical data processor with information relating to the detection of any unlawful data processing activities.

According to the GDPR 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 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 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 his or her tasks, which are:

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 Union or Member State data protection provisions;

b to monitor compliance with this Regulation, with other 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 referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

Pursuant to the data breach rules of the GDPR and of the Privacy Act, the DPO shall manage the data security incident register, which contains records of incidents and shall notify the DPA or the data subjects in some cases.

VI DISCOVERY AND DISCLOSURE

i Enforcement agencies

The DPA plays a key role in the enforcement of the protections of the GDPR and of the Privacy Act. The DPA has been appointed to act as a supervisory authority in the sense of the GDPR, therefore no separate agency has been created in Hungary for this purpose. The DPA is responsible both for the supervision and enforcement of compliance with the GDPR
and the Privacy Act and other data protection and data processing laws as well as freedom of information laws in Hungary. Hungarian data protection and privacy laws are enforced by the DPA and the Hungarian courts. No other organisations have an official role in data protection regulation.

The DPA monitors the conditions of the protection of personal data and investigates complaints. Representatives of the DPA may enter any premises where data are processed. If they observe any unlawful data processing, they have the authority to make the data controller discontinue the processing. The administrative procedure of the DPA is governed by the General Provisions of the Act on Administrative Procedure and, in the event of breach of the material provisions of the Act, the DPA is empowered to:

- request that an entity cease and desist from infringing the law;
- order the blocking, deletion or destruction of unlawfully processed data;
- prohibit the unlawful processing;
- suspend the transfer of data to foreign countries; and
- impose a fine of up to €20 million.

The GDPR appoints supervisory authorities to:

- monitor and enforce the application of the GDPR;
- promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention;
- advise, in accordance with Member State law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons’ rights and freedoms with regard to processing;
- promote the awareness of controllers and processors of their obligations under the GDPR;
- upon request, provide information to any data subject concerning the exercise of their rights under the GDPR and, if appropriate, cooperate with the supervisory authorities in other Member States to that end;
- handle complaints lodged by a data subject, or by a body, organisation or association, 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;
- cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of the GDPR;
- conduct investigations on the application of the GDPR, including on the basis of information received from another supervisory authority or other public authority;
- monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices;
- adopt standard contractual clauses;
- establish and maintain a list in relation to the requirement for data protection impact assessment;
- encourage the drawing up of codes of conduct and provide an opinion and approve such codes of conduct which provide sufficient safeguards;
encourage the establishment of data protection certification mechanisms and of data protection seals and marks and approve the criteria of certification;

where applicable, carry out a periodic review of certifications;

conduct the accreditation of a body for monitoring codes of conduct;

authorise contractual clauses and provisions;

approve binding corporate rules; and

keep internal records of infringements of the GDPR and of measures taken.

Under the GDPR and the Act, the data controller, data processor and data subject are all entitled to appeal to the court to contest an order of the DPA. Pending a final and binding decision of the court, the data concerned must not be erased or destroyed, but processing of the data must be suspended and the data blocked. Moreover, the general rights of appeal under the Civil Procedure Act will still apply.

The DPA may initiate criminal proceedings with the body authorised to launch such proceedings if it suspects that an offence has been committed during the course of the procedure. The DPA shall initiate infringement or disciplinary proceedings with the body authorised to launch such proceedings if it suspects that an infringement or disciplinary violation has been committed during the course of the procedure.

The Privacy Act has established the Conference of Internal Data Protection Officers, which is headed by the president of the DPA and secures the information exchange between data protection officers.

Recent enforcement cases

The DPA’s action plan is aimed at online stores and their data processing activities. Short summaries of some recent cases are below.

In one case,28 the DPA investigated the legitimacy of the cross-border data transfer practices of a company established in France. The company had implemented binding corporate rules (BCRs) to legitimise data transfers within the company group across the globe and subsequently filed these BCRs with the French Data Protection Authority (CNIL) for validation. Upon receiving CNIL approval, the company was listed on the relevant European Commission website as an entity using BCRs. The Hungarian DPA, however, detected *ex officio* that although the company had also requested approval for Hungary, it had failed to submit its BCRs to the local DPA for approval. Under the Privacy Act, BCRs may only be used as an adequate safeguard for international data transfers upon approval by the local DPA. The DPA established that, in the absence of local approval for the BCRs, the data transfers of the company had been unlawful and – without imposing any penalties – ordered the company to submit its BCRs to the Hungarian DPA without further delay.

In another case,29 the DPA investigated the data processing activities of a medium-sized company active in the consumer credit business. The DPA established that the company’s data-processing practices had been unlawful as the company had violated the principles of data minimisation and purpose limitation (by collecting and retaining copies of customer identification documents), had violated its obligations the concerning preliminary notification

---

28 NAIH/2016/5859/H.
29 NAIH/2017/1051/2/H.
of customers (by not informing customers on all aspects of the data processing) and had also processed customer personal data without a proper legal basis. Consequently, the DPA imposed a data protection fine amounting to 1 million forints.

Recently the DPA has rather focused on the enquiries of data controllers, data processors and data subjects concerning the implementation of the GDPR. Concerning these enquiries the DPA issues guidelines that are published on their website. Please find below some guidelines that can be considered as important or of general concern, albeit the DPA always emphasises that these guidelines are not enforceable and not binding:

Conciliation panels (e.g., panels mediating consumer protection cases) qualify as public authorities, therefore the rules of GDPR concerning public authorities shall be applied to these panels as well, including the obligation for the appointment of data protection officer.

Data protection registries may be kept in English language but in the case of a monitoring procedure by the supervisory authority it is the data controller’s duty to provide the Authority with adequate Hungarian translation.

iii Private litigation

In the event of infringement of his or her rights, a data subject may file a court action against a data controller. In the court proceeding, the data controller bears the burden of proving that the data processing was in compliance with the data protection laws.

In the event of harm to personal rights caused to the data subject in connection with data processing or breach of data security requirements, the data subject may plead before the courts for the controller to cease and desist from infringement, for satisfaction, as well as for the perpetrator to hand over financial gains made from the infringement. Moreover, since 15 March 2014, the data subject may also claim exemplary damages – namely lump sum damages that can be awarded by the court for the compensation of the harm by the data controller as a result of unlawful data processing or breach of data security requirements. Regarding the claim for exemplary damages, the data subject as a claimant does not need to evidence the harm beyond the breach of data protection laws.

Penalties imposed by the DPA are made public via its website.30 The DPA has imposed penalties three times between 25 August and 31 December 2016, and seven times in 2017 up to 1 September, while in 2018 fines have been imposed four times. The former maximum penalty of 20 million forints has not been imposed since September 2015; neither has the minimum amount of 100,000 forints. The amounts of imposed data protection fines since August 2016 have ranged from 300,000 to 15 million forints. Since the introduction of the new GDPR rules, the upper limits of the fines have seen a significant increase but no official actions have been completed since 25 May, therefore, it is yet to be seen how vigorous the fining practice of the DPA will be with the new rules.

VII PUBLIC AND PRIVATE ENFORCEMENT

The scope of the Hungarian Privacy Act and of the GDPR cover all kinds of data controlling and processing regarding the data of private persons, data of public interest or data that is public because of the public interest. The Hungarian Privacy Act is also applied if a data controller handling personal data is located outside the European Union and it commissions

30 www.naih.hu.
a data controller with a seat, business establishment, branch office, domicile or place of residence in Hungary, or uses a device located in Hungary, except when this device serves only to transit data traffic in the area of the European Union. If the Privacy Act applies, a data controller shall appoint a representative for the territory of Hungary.

The forwarding of personal data by an employer to a data processor located outside Hungary is not forbidden; however, it is subject to prior notification of the employee.

The new rules of the GDPR apply 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. The GDPR applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to (i) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union or (ii) the monitoring of their behaviour as far as their behaviour takes place within the Union.

This regulation creates a very wide territorial scope for the GDPR and for the supervisory authority enforcing the GDPR rules. However, it remains uncertain how supervisory authorities will have the resources to initiate investigations against foreign organisations.

VIII CYBERSECURITY AND DATA BREACHES

Hungary is a member of the Council of Europe’s Convention on Cybercrime, which was signed in 2001 in Budapest. A government decision was issued recently in which the basics of the National Cybersecurity Strategy of Hungary were laid down. In connection with this legal development, a series of other laws has been announced covering areas such as the electronic information security of the state and local governments, and the responsibilities of the National Electronic Information Security Authority and the National Cybersecurity Coordination Council. Critical systems and facilities have also been identified, and their special protection has been ordered by law.

In Hungary, the obligation to make reports in line with the European Union Agency for Network and Information Security guidelines only extends to the organs of public administration. However, private persons can also contact the Government Incident Response Team by email or telephone. A new Cybersecurity Strategy and Action Plan is planned to be created this year to clarify the tasks and scopes of responsibility of the state actors.

IX OUTLOOK

The EU General Data Protection Regulation has brought significant changes to the Hungarian data protection and privacy regime with effect from 25 May 2018 but taking into consideration the short period of time since its applicability, it is hard to assess its actual short and long-term effects.
I OVERVIEW

A decidedly inadequate collection of statutes currently governs cybersecurity and data protection in India. Authorities constituted to regulate compliance and enforce penalties for non-compliance under the Information Technology Act 2000 and the Information Technology (Amendment) Act 2008 have been inactive for years, and very little significant jurisprudential development has occurred on the subjects of cybersecurity, privacy and data protection over the past few years. In 2013, the then government drafted a National Cybersecurity Policy, which generated considerable interest both in India as well as abroad, particularly in view of India’s position as an exponentially growing business process outsourcing destination. Sadly, progress on the policy was stymied for reasons that have not been made public, reflecting rather poorly on the government’s intention to provide clear, robust and watertight law on these matters.

The foregoing is not to say that the urgent need for change in this respect has not been recognised. In July 2016 the Joint Secretary for Cyber Laws and E-Security, R K Sudhanshu, stated to the press that the government is in the process of developing new encryption and cybersecurity policies as part of a thorough overhaul of the law regulating cybersecurity in India.2

In 2017, the Minister for Law and IT, Ravi Shankar Prasad, said that the government is finalising cybersecurity standards for mobile phones and has already issued notice to most smartphone manufacturers asking them to furnish details related to cybersecurity.3

Following the government launch, in 2015, of a heavily advertised campaign called Digital India, the major agenda of which was to create ‘digital infrastructure’ to facilitate the digital delivery of services and increase digital literacy, the prime minister has been involved in an aggressive attempt to compensate for lost time as regards the enhancement of cybersecurity. Digital India triggered major investment flows into the technology sector, and the campaign has caused questions to be raised in the media and academia about privacy and the protection of data, which will hopefully spur the government on to legislate more clearly and in detail on these subjects.

1 Aditi Subramaniam is an associate principal and Sanuj Das is a managing associate at Subramaniam & Associates.
Subsequently, 2016 was a mixed bag of both encouraging and slightly disturbing developments, although notably none of these developments resulted in the substantive renovation or repair of statutory law, as has been repeatedly promised by the authorities for several years, with the exception of the introduction of the Aadhar Act, to provide targeted delivery of financial benefits.

The Aadhar Act was challenged in a series of petitions that questioned its constitutional validity. A moot question raised in these petitions was whether privacy is a fundamental right guaranteed under the Constitution of India. The verdict on these petitions was delivered this year by a nine-judge constitutional bench of the Supreme Court, which held privacy to be a fundamental right of every citizen under the Constitution.4

In addition to the litigious developments described above, 2017 saw the government amending the Income Tax Act 1961–2017 to make it mandatory for taxpayers to link their Permanent Account Numbers (PANs) to file income-tax returns, open bank accounts and conduct financial transactions beyond a threshold, to curb tax evasion and money laundering. The Department of Telecommunications has also mandatorily sought to use the Aadhar Act as a tool for subscriber verification from existing mobile telephone subscribers and made it mandatory for new connections.5 The policies of the government were criticised and challenged in the Supreme Court, which has reserved a verdict that is expected later in 2018.

While the developments of previous years set the tone for 2018, an impetus to make specific data protection legislation came with a private member’s bill — the Data Privacy Bill 2017 — and the release of Justice BN Srikrishna Committee’s recommendations.6 These developments are discussed in detail below.

II THE YEAR IN REVIEW

The following major developments of note occurred in the course of the past year, and these affect national policy, legislation and jurisprudence on cybersecurity, data protection and privacy to varying degrees.

i Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act 2016 (the Aadhar Act)

The government pushed the Aadhar Bill through Parliament in a week in March 2016, resulting in the Aadhaar Act. Briefly, the Act provides for the issuance of an identification number issued by the Unique Identification Authority of India to citizens of the country. This number will be used to deliver state subsidies directly into the hands of beneficiaries.

The Aadhaar scheme was first mooted as the Indian equivalent to the social security number in the United States. The passage of this bill into law has, however, generated furious debate about the privacy concerns it necessarily raises — the Act envisages the creation of a database of personal identifying information of potentially a billion unsuspecting citizens, and also the use of the data therein to facilitate mass surveillance, and absolutely no framework or

legislation is in place to regulate either the former or the latter. The Act contains provisions on the strict limitation on sharing the data collected, but also makes rather large exceptions to these limitations that are a major cause for concern.7

In a writ petition before the apex court of the country, the Aadhar Act was challenged as being ultra vires in relation to the Constitution owing to its severe violation of citizens’ fundamental right to privacy. It was put to the court that the Aadhar Act coerces individuals to part with their personal information, including biometric details, and creates an environment that can be used for surveillance. While the fate of the Aadhar Act is still undecided, one of the biggest hurdles in the matter has been resolved by the Supreme Court in a landmark judgment. A nine-judge constitution bench, presided over by the Chief Justice of India, was posed the question of whether privacy is in fact a fundamental right guaranteed under the Constitution.

The Court ruled on this question in the affirmative and in doing so observed that it is not an absolute right but one subject to certain reasonable restrictions. On the data protection aspect, the Court observed that the right of an individual to exercise control over his or her personal data and to be able to control his or her own life would also encompass the right to control his or existence on the internet. The judgment also states that consent obtained from users has to be informed consent, given in an informed manner by users, and cannot be shrouded in lengthy agreement terms, The Court even upheld the right of an individual to be forgotten from the internet by observing that:

If we were to recognise 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.

The Supreme Court resumed hearing on the constitutional validity of the Aadhar Act itself in May 2018 and after a marathon hearing lasting 38 days, reserved its judgment. Among other issues, the Supreme Court’s judgment will shed light on whether the government is entitled to collect citizens’ biometric and demographic data and the manner in which it is entitled to do so.

ii WhatsApp litigation and Justice BN Srikrishna Committee

In widely publicised litigation in the public interest against WhatsApp, the privacy policies of WhatsApp and Facebook were called into question. This case is discussed in more detail in Section VII.iii.

India

iv India selected as a member of the UN group of governmental experts (GGE) to identify ‘rules of the road’ for cyberspace

India has been selected to be a member of the 2016 GGE set up to identify ‘rules of the road’ for cyberspace. While the GGE’s report is endorsed by the General Assembly, it is not officially binding. However, in combination with the initiation of the US–India Cyber Relationship, India’s participation in the 2016 GGE meeting signifies a way forward in the framing of issues that must be addressed in these matters.

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

In the absence of specific legislation, data protection is achieved in India through the enforcement of privacy rights on the basis of a patchwork of legislation, as follows.

The Information Technology Act (2000) (IT Act) and the Information Technology (Amendment) Act 2008

The IT Act contains provisions for the protection of electronic data. The IT Act penalises ‘cyber contraventions’ (Section 43(a)–(h)), which attract civil prosecution, and ‘cyber offences’ (Sections 63–74), which attract criminal action.

The IT Act was originally passed to provide legal recognition for e-commerce and sanctions for computer misuse. However, it had no express provisions regarding data security. Breaches of data security could result in the prosecution of individuals who hacked into the system, under Sections 43 and 66 of the IT Act, but the Act did not provide other remedies such as, for instance, taking action against the organisation holding the data. Accordingly, the IT (Amendment) Act 2008 was passed, which, inter alia, incorporated two new sections into the IT Act, Section 43A and Section 72A, to provide a remedy to persons who have suffered or are likely to suffer a loss on account of their personal data not having been adequately protected.

The Information Technology Rules (the IT Rules)

Under various sections of the IT Act, the government routinely gives notice of sets of Information Technology Rules to broaden its scope. These IT Rules focus on and regulate specific areas of collection, transfer and processing of data, and include, most recently, the following:

a the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules,9 which require entities holding users’ sensitive personal information to maintain certain specified security standards;

b the Information Technology (Intermediaries Guidelines) Rules,10 which prohibit content of a specific nature on the internet, and an intermediary, such as a website host, is required to block such content;

---

8 Links to pdf versions of the IT Act and Rules are available on the website of the Ministry of Electronics and Information Technology: meity.gov.in/content/cyber-laws.
c the Information Technology (Guidelines for Cyber Cafe) Rules,\(^{11}\) which require cybercafes to register with a registration agency and maintain a log of users’ identities and their internet usage; and

d the Information Technology (Electronic Service Delivery) Rules,\(^{12}\) which allow the government to specify that certain services, such as applications, certificates and licences, be delivered electronically.

The IT Rules are statutory law, and the four sets specified above were notified on 11 April 2011 under Section 43A of the IT Act.

Penalties for non-compliance are specified by Sections 43 and 72 of the IT Act.

In 2011 and subsequently in 2014, draft versions of a proposed law referred to as the Privacy Bill were released on the internet by a non-profit organisation called the Centre for Internet and Society, which claimed that these drafts had been leaked by the Department of Electronics and Information Technology.\(^{13}\) The Privacy Bill recognises an individual’s right to privacy, but states also that certain circumstances, including protection of national integrity or sovereignty, national security, prevention of crime and public order, warrant the invasion of that privacy. In May 2016, the Minister for Communications and Information Technology, Ravi Shankar Prasad, stated in the upper house of Parliament that the government is still working on the proposed law.\(^{14}\)

Additional legislation

In addition to the legislation described above, data protection may also sometimes occur through the enforcement of property rights based on the Copyright Act (1957). Further, other legislation such as the Code of Criminal Procedure (1973), the Indian Telegraph Act 1885, the Companies Act (1956), the Competition Act (2002) and, in cases of unfair trade practices, the Consumer Protection Act (1986), would also be relevant. Finally, citizens may also make use of the common law right to privacy, at least in theory – there is no significant, recent jurisprudence on this.

A Data (Privacy and Protection) Bill 2017 (the Data Privacy Bill 2017) was introduced in Parliament in July 2017 by a private member. Apart from intending to make the 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 the regulation and adjudication of privacy-related disputes. It is yet to be enacted into law.

Compliance regulators

CERT-In

Under Section 70B of the IT (Amendment) Act 2008, the government constituted CERT-In, which the website of the Ministry of Electronics and Information Technology refers to as the ‘Indian Computer Emergency Response Team’. CERT-In is a national nodal agency responding to computer security incidents as and when they occur. The Ministry of Electronics and Information Technology specifies the functions of the agency as follows:

\(^{11}\) meity.gov.in/sites/upload_files/dit/files/GSR315E_10511(1).pdf.
\(^{12}\) meity.gov.in/sites/upload_files/dit/files/GSR316E_10511(1).pdf.
\(^{14}\) www.medianama.com/2016/05/223-government-privacy-draft-policy.
a. collection, analysis and dissemination of information on cybersecurity incidents;

b. forecast and alerts of cybersecurity incidents;

c. emergency measures for handling cybersecurity incidents;

d. coordination of cybersecurity incident response activities; and

e. issuance of guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response to and reporting of cybersecurity incidents.15

**Cyber Regulations Appellate Tribunal (CRAT)**

Under Section 48(1) of the IT Act 2000, the Ministry of Electronics and Information Technology established CRAT in October 2006. The IT (Amendment) Act 2008 renamed the tribunal Cyber Appellate Tribunal (CAT). Pursuant to the IT Act, any person aggrieved by an order made by the Controller of Certifying Authorities, or by an adjudicating officer under this Act, may prefer an appeal before the CAT. The CAT is headed by a chairperson who is appointed by the central government by notification, as provided under Section 49 of the IT Act 2000.

Before the IT (Amendment) Act 2008, the chairperson was known as the presiding officer. Provisions have been made in the amended Act for CAT to comprise of a chairperson and such a number of other members as the central government may notify or appoint.16

**Definitions**

The legislation does not contain a definition of ‘personal data’. The IT Rules do define personal information as any information that relates to a natural person that, 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.

Further, the IT Rules define ‘sensitive personal data or information’ as personal information consisting of information relating to:

- passwords;
- financial information, such as bank account, credit card, 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 the provision of services; or
- any information received under the above clauses by a body corporate for processing, or that has been stored or processed under lawful contract or otherwise.

Provided that any information is freely available or accessible in the public domain, or furnished under the Right to Information Act 2005 or any other law for the time being in force, it shall not be regarded as sensitive personal data or information for the purposes of these rules.

---

15 www.cert-in.org.in.

The draft of the proposed Privacy Bill 2011 defines ‘personal data’ as any data that 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.

The Data Privacy Bill 2017 also defines ‘sensitive personal data’ as follows:

- unique identifiers such as the Aadhar number or personal account number;
- physical and mental health, including medical history;
- biometric or genetic information;
- criminal convictions;
- banking credit and financial data; and
- narco analysis or polygraph test data.

The Privacy Bill 2011 and Data Privacy Bill 2017 contains more specific definitions of the above terms, and also defines concepts not found in the current legislation, such as ‘processing’, ‘data controller’ and ‘data processor’.

ii General obligations for data handlers

Obligations for data processors, controllers and handlers

Transparency

The IT Rules state that all data handlers must create a privacy policy to govern the way they handle personal information. Further, the policy must be made available to the data subject who is providing this information under a lawful contract.

Lawful basis for processing

A body corporate (or any person or entity on its behalf) cannot use data for any purpose unless it receives consent in writing from the data subject to use it for that specific purpose. Consent must be obtained before collection of the data. The IT Rules also mandate that sensitive personal information may not be collected unless it is connected to the function of the corporate entity collecting it, and then only if the collection is necessary for that function. It is the responsibility of the body corporate to ensure that the sensitive personal information thus collected is used for no other purpose than the one specified.

Purpose limitation

Neither the IT Rules nor the IT Act specify a 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 retention

Legislation is yet to be clarified on specific rules with respect to the retention of data by data processors or handlers. 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:

- it is required by law to be retained for a longer period;
- the data subject consents to its retention for a longer period;
such retention is required by a contract between the data subject and the data controller; or

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.

**Registration formalities**

India currently does not have any legislative requirements with respect to registration or notification procedures for data controllers or processors. However, the draft Privacy Bill proposes to change this by introducing not only specific registration criteria and formalities, but also sanctions for failure to register.

**Rights of individuals**

**Access to 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. This situation will be clarified somewhat by the proposed Privacy Bill 2011, 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.

**Correction and deletion**

Rule 5, Subsection 6 of the IT Rules states that data subjects must be allowed access to the data provided by them and to 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 that 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 in *KS
Puttaswamy & Ors v. Union of India & Ors*[^17] also identified the right to be forgotten, in
physical and virtual spaces such as the internet, under the umbrella of informational privacy.

**Objection to processing and marketing**

Rule 5 of the IT Rules states that the data subject or provider of information shall have the
option to later withdraw consent that may have been given to the corporate entity previously,
and the withdrawal of consent must be stated in writing to the body corporate. On withdrawal
of consent, the corporate body is prohibited from processing the personal information in
question. In the case of the data subject not providing consent, or later withdrawing consent,
the corporate body 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.

**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 disclosure has already been agreed to in the contract between the data subject and the
data controller; or 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 verification of identity; prevention, detection and investigation of crime; or
prosecution or punishment of offences.

Recipients of this sensitive personal information are prohibited from further disclosing
the information.

Right to complain to the relevant data protection authority

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.

iii Specific regulatory areas

Financial privacy

Public Financial Institutions (Obligation as to Fidelity and Secrecy) Act 1983

Under this Act, public financial institutions are prohibited from divulging any information relating to the affairs of their clients except in accordance with laws of practice and usage.

The Prevention of Money Laundering Act 2002

The Prevention of Money Laundering Act (PMLA) was passed in an attempt to curb money laundering and prescribes measures to monitor banking customers and their business relations, financial transactions, verification of new customers, and automatic tracking of suspicious transactions. The PMLA makes it mandatory for banking companies, financial institutions and intermediaries to furnish to the Director of the Financial Intelligence Unit (under the PMLA) information relating to prescribed transactions, and which can also be shared, in the public interest, with other government institutions or foreign countries for enforcement of the provisions of the PMLA or through exchanges of information to prevent any offence under the PMLA.

Credit Information Companies (Regulation) Act 2005 and The Credit Information Companies Regulations 2006

This legislation is essentially aimed at regulation of sharing and exchanging credit information by credit agencies with third parties. Disclosure of data received by a credit agency is prohibited, except in the case of its specified user and unless required by any law in force.

The regulations prescribe that the data collected must be adequate, relevant, and not excessive, up to date and complete, so that the collection does not intrude to an unreasonable extent on the personal affairs of the individual. The information collected and disseminated is retained for a period of seven years in the case of individuals. Information relating to criminal offences is maintained permanently while information relating to civil offences is retained for seven years from the first reporting of the offence. In fact, the regulations also prescribe that personal information that has become irrelevant may be destroyed, erased or made anonymous.

Credit information companies are required to obtain informed consent from individuals and entities before collecting their information. For the purpose of redressal, a complaint can be written to the Reserve Bank of India.

**Payment and Settlement Systems Act 2007**

Under this Act, the Reserve Bank of India (RBI) is empowered to act as the overseeing authority for regulation and supervision of payment systems in India. The RBI is prohibited from disclosing the existence or contents of any document or any part of any information given to it by a system participant.

**Foreign Contribution Regulation Act 2010**

This Act is aimed at regulating and prohibiting the acceptance and utilisation of foreign contributions or foreign hospitality by certain individuals, associations or companies for any activities detrimental to the national interest and, under the Act, the government is empowered to call for otherwise confidential financial information relating to foreign contributions of individuals and companies.

**Workplace privacy**

In the present scenario, employers are required to adopt security practices to protect sensitive personal data of employees in their possession, such as medical records, financial records and biometric information. In the event of a loss to an employee due to lack of adequate security practices, the employee would be entitled to compensation under Section 43A of the Information Technology Act 2000. Other than this piece of legislation, there is no specific legislation governing workplace privacy, although, in relation to the workplace, the effect of the Supreme Court judgment on privacy as a fundamental right remains to be seen.

**Children’s privacy**

Section 74 of the Juvenile Justice (Care and Protection of Children) Act 2015 mandates that the name, address or school, or any other particular, that may lead to the identification of a child in conflict with the law or a child in need of care and protection or a child victim or witness of a crime shall not be disclosed in the media unless the disclosure or publication is in the child’s best interest.

**Health and medical privacy**

**Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations 2002 (Code of Ethics Regulations 2002)**

Under these regulations, physicians are obliged to protect the confidentiality of patients during all stages of procedures, including information relating to their personal and domestic lives unless the law mandates otherwise or there is a serious and identifiable risk to a specific person or community of a notifiable disease.

---

22 https://fcraonline.nic.in/home/PDF_Doc/FC-RegulationAct-2010-C.pdf.
Medical Termination of Pregnancy Act 1971
This Act prohibits the disclosure of matters relating to treatment for termination of pregnancy to anyone other than the Chief Medical Officer of the state. The register of women who have terminated their pregnancy, as maintained by the hospital, must be destroyed on the expiry of a period of five years from the date of the final entry.

Ethical Guidelines for Biomedical Research on Human Subjects
These Guidelines require investigators to maintain confidentiality of epidemiological data. Data of individual participants can be disclosed in a court of law under the orders of the presiding judge if there is a threat to a person’s life, allowing communication to the drug registration authority in cases of severe adverse reaction and communication to the health authority if there is risk to public health.

iv Technological innovation and privacy law
There are no marketing restrictions on the internet or through email. Because India has no comprehensive data protection regime, issues such as cookie consent have not yet been addressed by Indian legislation.

The IT Rules provide reasonable security practices to follow as statutory security procedures for corporate entities that collect, handle and process data, and these also apply to the use of big data. Unfortunately, no specific guidelines exist for the use of big data and big-data analytics in India.

IV INTERNATIONAL DATA TRANSFER AND DATA LOCALISATION
Despite India’s dogged attempts to join the APEC for several years, its inclusion on the forum has so far been limited to observer status. APEC rules therefore do not apply in the Indian jurisdiction thus far.

In terms of restrictions on transfer of data, 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 the transferee ensures the same level of data protection that the body corporate maintained, as required by the IT Rules. A data transfer is only allowed if it is required for the performance of a lawful contract between the data controller and the data subjects; or the data subjects have consented to the transfer.

The proposed Privacy Bill, if enacted, will place slightly more stringent restrictions on international transfers of personal data.

As worded, Section 7 is already rather restrictive. However, in some ways this is no different from EU data protection legislation, which restricts transfers of personal data outside the EU unless certain measures are taken, such as requiring the data importer to sign up to EU Model Contract Clauses. In addition, the Ministry of Information Technology clarified via a press note released on 24 August 2011 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 may subscribe to whichever secure methods of data transfer they prefer, provided that the transfer in question does not violate any law either in India or in the country the data are being transferred to. Presumably litigation in this sector – so far non-existent – will further clarify matters.
In general, data protection laws in India apply to businesses established in other jurisdictions as well. 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 or her nationality, if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

V COMPANY POLICIES AND PRACTICES

The general obligations for data handlers elaborated above apply to all companies handling data, and their policies must reflect as much. In addition, the IT Rules contain specific legislation to deal with best practices, particularly in the context of breach and security.

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 and 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 with the nature of business. 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.


3. Any industry association or an entity formed by such an association, whose members are self-regulating by following other than IS/ISO/IEC codes of best practices for data protection as per sub-rule (1), shall get its codes of best practices duly approved and notified by the Central Government for effective implementation.

4. The body corporate or a person on its behalf who have implemented either IS/ISO/IEC 27001 standard or the codes of best practices for data protection as approved and notified under sub-rule (3) shall be deemed to have complied with reasonable security practices and procedures provided that such standard or the codes of best practices have been certified or audited on a regular basis by entities through independent auditor, duly approved by the Central Government. The audit of reasonable security practices and procedures shall be carried out by an auditor at least once a year or as and when the body corporate or a person on its behalf undertake significant upgradation of its process and computer resources.

There are no statutory registration or notification requirements for either data processors or data controllers. The proposed Privacy Bills provide for the establishment of a Data Protection Authority of India, and 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 determined by the central government.
VI DISCOVERY AND DISCLOSURE

If 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 an Indian court is likely to enforce the request in India. In the absence of a court order, however, no obligation exists against an Indian company to make any kind of disclosure.

In a Ministry of Communications and Information Technology press release, the government clarified that any Indian outsourcing service provider or 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 the IT Rules requirements with respect to disclosure of information or consent, provided it does not have direct contact with the data subjects when providing services.

See also the exceptions to the consent requirements for disclosure detailed in Section III.ii.

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

In addition to the security practices and policies outlined in Section V, and as mentioned in Section III.i, the proposed Privacy Bill conceptualises the creation of a data protection authority for the enforcement of data protection legislation and to oversee compliance with it. The Privacy Bill will override the IT Rules if it is enacted, and in that event, its provisions pertaining to the security of personal data that state specifically that every data controller must set appropriate technological, organisational and physical standards for the security of data under its control will also come into force.

ii Recent enforcement cases

As is evident from the above, India has no distinct legislative framework to support litigation in the areas of privacy, cybersecurity and data protection. There has been no significant litigation in this area in the recent past. It is to be hoped that with the passage of the Privacy Bill into law and a clearer definition of rights in this sector, the enforcement of rights will become both more active and more stringent.

iii Private litigation

Karmanyaa Singh Sareen & Anr v. UOI & Ors

This case was filed before the High Court of New Delhi in the public interest by two university students against WhatsApp, Facebook and the Union of India (through the Department of Telecommunications (DoT) and the Telecom Regulatory Authority of India (TRAI)). Subsequent to its acquisition by Facebook, WhatsApp updated its privacy policy in August 2016.

24 (WP(C) 7663/2016): lobis.nic.in/ddir/dhc/GRO/judgement/24-09-2016/GRO23092016CW76632016.pdf.
2016, stating that it would now share a limited amount of user information with Facebook for optimised advertising and networking suggestions. The petitioners contended that this change in policy compromised the privacy of the users of WhatsApp.

On 23 September 2016, the High Court of New Delhi passed an order directing WhatsApp to ‘scrub’ all user data collected prior to 25 September for users who chose to opt out of the service prior to this date. For users choosing to continue to make use of the service, the High Court directed that only data collected after 25 September could be shared by WhatsApp with Facebook and its group companies. The Court also directed DoT and TRAI to examine the feasibility of bringing WhatsApp (and other internet-based messaging applications) under a statutory regulatory framework, ordering that these respondents must take an appropriate decision on this matter ‘at the earliest’.

This decision is significant in that it is the only emphatic recognition of the right to privacy for individuals that our jurisprudence has seen in the past few years, other than the landmark Supreme Court judgment striking down Section 66A of the IT Act in 2015. In 2017, the petitioners filed an appeal before the Supreme Court challenging the order of the High Court. The petitioners impugned the directions of the High Court and sought directions of the Supreme Court since, according to the petitioners, the policy formulated by WhatsApp was unconscionable and unacceptable. The Supreme Court is still hearing the matter and it seems unlikely that the controversy will be resolved this year as well. However, pursuant to the KS Puttaswamy judgment in 2017 – holding privacy a fundamental right – the Supreme Court had constituted the Justice BN Srikrishna Committee to identify key data protection issues in India and recommend methods of addressing them. The Committee released its recommendations in August 2018, some of the salient recommendations being:

\[\begin{align*}
  a & \text{ the establishment of an autonomous body, styled the Arbitration Promotion Council of India (APCI), having representatives from all stakeholders for grading arbitral institutions in India;} \\
  b & \text{ the recognition of professional institutes by the APCI, providing for the accreditation of arbitrators;} \\
  c & \text{ training workshops and interactions with law firms and law schools organised by the APCI to train advocates with an interest in arbitration, with the goal of creating a specialist arbitration bar;} \\
  d & \text{ the creation of a specialist arbitration bench within courts to deal with such commercial disputes;} \\
  e & \text{ various provisions of the 2015 Amendments in the Arbitration and Conciliation Act intended to make arbitration faster and more efficacious and incorporate international best practices.}
\end{align*}\]

Finally, the Committee released the draft of the Personal Data Protection Bill 2018, which if implemented, could address the issue around privacy of personal information in India. Among other important inclusions, the Personal Data Protection Bill draft puts an emphasis on informed user consent for the processing of personal data and enshrines the right to be forgotten.
KS Puttaswamy & Ors v. Union of India & Ors

In **KS Puttaswamy & Ors v. Union of India & Ors**, and litigation that followed it, the constitutional validity of the Aadhar Act scheme was challenged on the grounds that it was *ultra vires* in relation to the Constitution and violated the rights of every citizen.

The matter was initially heard by a three-judge bench, which referred it to a five-judge bench. However, owing to previous judgments by larger benches of the Supreme Court, a nine-judge bench was constituted to address the issue of whether privacy was a fundamental right guaranteed under the Constitution. The nine-judge bench gave a unanimous decision holding privacy to be a fundamental right of every citizen of the country, with qualified riders. In fact, the judgment acknowledges neo-libertarian values, such as the right to be forgotten, and will go down as a landmark judgment. The challenge to the constitutional validity of the Aadhar Act itself is still pending and a judgment of the Supreme Court in this matter is expected soon.

**VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS**

Unfortunately, Indian jurisprudence sheds no light on compliance requirements for organisations functioning outside India (see Section IV).

**IX CYBERSECURITY AND DATA BREACHES**

See Sections V and VI for information on breaches and breach reporting requirements. In addition to the information given in those sections, it is pertinent to note that in the context of a legal requirement to report data breaches to individuals, while the law as it is contains no such provision, the draft Privacy Bill does. In fact, the draft exempts the data protection authority from this requirement in only two scenarios: if the data protection authority believes that such a notification will impede a criminal investigation or the identity of the data subject cannot possibly be identified.

Earlier this year it emerged that Cambridge Analytica – a political consultancy firm – harvested social media giant Facebook’s users’ data without consent to influence elections. Indian authorities have indicated that the Cambridge Analytica will be investigated to ascertain the nature of its work in India.26

**X OUTLOOK**

There is no doubt that India urgently needs to take a keen look at its poorly regulated digital spaces and at the virtual activities of individuals, private organisations and governmental authorities alike. The several agencies performing cybersecurity operations in India, such as the National Technical Research Organisation, the National Intelligence Grid and the National Information Board, require robust policy and legislative and infrastructural support from the Ministry of Electronics and Information Technology, and from the courts, to enable them to do their jobs properly. The EU’s General Data Protection Regulation may provide impetus for India in this regard, particularly given that not only will the regulation affect

---


cross-border information flow (and India is a net information exporter), but also the EU has exposed several lacunae in the standards applied by the Indian government to the protection of data and enforcement of cybersecurity in a report following approval of its new data protection regulation. While it seems that the government is concerned and keen to bring about change in this sector, in view of India's rather poor record in prioritising these matters, optimism is not necessarily warranted at this stage.
Chapter 15

IRELAND

Anne-Marie Bohan

I OVERVIEW

The data protection regime in Ireland is governed by the Data Protection Acts 1988 and 2003 (DPA), which transposed European Directive 95/46/EC on data protection (the Directive) into Irish law. In addition, there are numerous sector-specific regulations in areas such as employment, electronic communications, health data and genetic data. Ireland protects privacy and data protection rights fundamentally at a constitutional level in Articles 40.3.1, 40.3.2 and 40.5 of the Irish Constitution. These rights are balanced against the freedom of expression protected in Article 40.6 and none are regarded as absolute.


II THE YEAR IN REVIEW

It has been an eventful year for data protection in Ireland. The Court of Justice of the European Union (CJEU) struck down the US–EU Safe Harbor Framework in October 2015 following a reference from the Irish High Court. This decision precipitated the EU

---

1 Anne-Marie Bohan is a partner at Matheson. The information in this chapter was accurate as of October 2016 and the author wishes to thank Andreas Carney, who no longer works at the firm, for his contribution to the chapter.
2 SI No. 337 of 2014 – Data Protection Act 1988 (Commencement) Order 2014 and SI No. 338 of 2014 – Data Protection (Amendment) Act 2003 (Commencement) Order 2014. These make it unlawful for employers to require employees or applicants for employment to make an access request seeking copies of personal data that are then made available to employers or prospective employers. This provision also applies to any person who engages another person to provide a service.
3 SI No. 336/2011 – European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (E-Privacy Regulations). This deals with specific data protection issues relating to use of electronic communication devices and particularly with direct marketing restrictions.
4 SI No. 82/1989 – Data Protection (Access Modification) (Health) Regulations, 1989. This outlines certain restrictions in the right of access relating to health data.
Commission and US Department of Commerce agreement in July of this year on a new framework for trans-Atlantic data transfers in the form of the EU–US Privacy Shield. While the Privacy Shield has its critics, it now offers another means of legitimately transferring personal data to the United States.

The ability of US authorities to legitimately access personal data held in Ireland was tested in Microsoft Corporation v. United States of America in which US authorities sought to compel Microsoft to disclose emails located in their Dublin-based data centre as part of a narcotics investigation. While an initial decision ruled in favour of the US authorities, the Second US Circuit Court of Appeals overturned that decision and determined that the relevant US statute being relied on by the authorities did not have extraterritorial effect and so did not empower them to require the production of personal data held in Ireland. This decision was largely welcomed, as it gave a level of certainty to those data controllers who strategically host personal data only within Ireland and other European Economic Area (EEA) Member States.

The year also saw the Office of the Data Protection Commissioner (ODPC) reopen an office in Dublin and also increase its headcount. The ODPC’s annual report for 2015 shows a slight decrease in the number of complaints opened for investigation and breach notifications made to the office, as well as highlighting prosecutions undertaken. According to the ODPC, the largest single category of complaints related to data subject access rights, which accounted for over 60 per cent of the total number of complaints in 2015.

### III REGULATORY FRAMEWORK

#### i Privacy and data protection legislation and standards

As well as conferring rights on individuals, the DPA also place obligations on those who collect and process personal data. The DPA seek to regulate the collection, processing, keeping, use and disclosure of personal data. The DPA place responsibilities on both data controllers and, to a lesser extent, on data processors.

The E-Privacy Regulations provide for a number of protections and offences in relation to electronic communications and, in particular, direct marketing via electronic means.

The key definitions under the DPA are as follows:

- **personal data**: data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller;

- **sensitive personal data**: personal data as to:
  - the racial or ethnic origin, the political opinions or the religious or philosophical beliefs of the data subject;
  - whether the data subject is a member of a trade union;
  - the physical or mental health or condition or sexual life of the data subject;
  - the commission or alleged commission of any offence by the data subject; or
  - any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings;

---

8 Electronic Communication Privacy Act 1986.

9 The ODPC Report notes 932 complaints that were opened for investigation in 2015 and 960 such complaints in 2014.
processing: in relation to information or data, the performing of any operation or set of operations on the information or data, whether by automatic or other means, including:
• obtaining, recording or keeping the information or data;
• collecting, organising, storing, altering or adapting the information or data;
• retrieving, consulting or using the information or data;
• disclosing the information or data by transmitting, disseminating or otherwise making it available; and
• aligning, combining, blocking, erasing or destroying the information or data;

data controller: a person who, either alone or with others, controls the contents and use of personal data;

data processor: a person who processes personal data on behalf of a data controller, but this does not include an employee of a data controller who processes such data in the course of his or her employment; and

data subject: an individual who is the subject of personal data.

General obligations for data handlers

Obligations of data controllers

The general obligations on data controllers are as follows.

Transparency

Data subjects must be provided with information relating to the processing of their data. This includes:

a. the identity of the data controller or their representative, the data processor, or both;

b. the purposes for which the data are intended to be processed; and

c. any other information that is necessary, having regard to the specific circumstances in which data are to be processed, including but not limited to details of recipients or categories of recipients of the personal data and information as to the existence of the right of access and the right to rectify data.

Lawful basis for processing

At least one of the following is required for personal data to be lawfully processed:

a. consent of the data subject (specific, freely given, informed); or

b. the processing is necessary:
• for the performance of a contract to which the data subject is a party;
• to take steps at the request of the data subject prior to entering into a contract;
• for compliance with a legal obligation to which the data controller is subject (other than an obligation imposed by contract);
• to prevent injury or other damage to the health of the data subject or serious loss or damage to property of the data subject, or to otherwise to protect his or her vital interests where the seeking of the consent of the data subject is likely to result in those interests being damaged;
• for compliance with a legal obligation, including the administration of justice; for the performance of a function conferred on a person by law; for the performance

Sensitive personal data must also pass an additional legitimate basis for processing.
of a function of the government or a minister of the government; or for the performance of any other function of a public nature that is performed in the public interest; or

- for the purposes of legitimate interests pursued by the data controller (or a third party to whom the personal data are disclosed), provided that the rights of the data subject are not unduly prejudiced.

**Purpose limitation**

Personal data should only be obtained for one or more specified, explicit and legitimate purposes, and should not be further processed in a manner incompatible with those purposes.

**Proportionality**

Personal data collected must be adequate, relevant and not excessive in relation to the purposes for which they are collected or are further processed.

**Retention**

Personal data should not be kept for longer than is necessary for the purpose for which they were obtained. If the purpose for which the information was obtained has ceased and the personal information is no longer required, the data must be deleted or disposed of in a secure manner.

**Rights of data subjects**

The general rights of data subjects are as follows.

**Access to data**

Data subjects have the right to, free of charge, find out if an organisation or an individual holds information about them. This includes the right to be given a description of the personal data and to be told the purposes for which the data are held. A request for these data must be made in writing by the data subject and the individual must receive a reply within 21 days according to the DPA.

Data subjects have the right to obtain a copy, within 40 days of a request, of any personal data that relate to them that are held either on a computer or in a structured manual filing system, or that are intended for such a system.

A number of exceptions to the right of access exist under the DPA, including legal privilege, research data, data that comprise an opinion given in confidence (subject to certain limitations) or data used for the investigation of offences.

**Correction and deletion**

Data subjects have the right to request in writing to have their data either deleted or corrected where the data are not obtained lawfully or are inaccurate. The data controller or processor must respond within a reasonable amount of time and no later than 40 days after the request. There is no express right of a data subject to request the deletion of their information if they are being processed lawfully.
Objection to processing

Data subjects have the right to object to processing that is likely to cause damage or distress. This right applies to processing that is necessary for the purposes of legitimate interests pursued by the data controller to whom the personal data are or will be disclosed, or processing that is necessary for the performance of a task carried out in the public interest or in the exercise of official authority.

Objection to marketing

Data subjects have the right, by written request, to require a data controller to cease processing data for that purpose and, where they are only retained for that purpose, they have the right to have it erased. The data controller must do this within 40 days.

Under the E-Privacy Regulations, data subjects have the right to have their ‘opt-out’ preference recorded in the National Directory Database, which constitutes an objection to direct telephone marketing to them.

Complaint to relevant data protection authority or authorities

Data subjects have a right of complaint to the ODPC in relation to the treatment of their personal data. The ODPC must investigate such complaints unless it considers them to be ‘frivolous or vexatious’.

Registration

It is obligatory for the following types of data controller to register with the ODPC if they hold personal data:

- government bodies and public authorities;
- banks, financial and credit institutions and insurance undertakings;
- data controllers whose business consists wholly or mainly of direct marketing;
- data controllers whose business consists wholly or mainly in providing credit references;
- data controllers whose business consists wholly or mainly in collecting debts;
- internet access providers, telecommunications networks and service providers;
- data controllers that process genetic data (as specifically defined in Section 41 of the Disability Act 2005); and
- health professionals processing personal data related to mental or physical health.

Data processors that process personal data on behalf of a data controller in any of the categories listed above must also register.

Exemptions

Generally, all data controllers and processors must register unless an exemption applies, either under Section 16(1)(a) or (b) of the DPA or under SI No. 657 of 2007. Under Section 16(1)(a) or (b) of the DPA, the following are excluded from registration:

- organisations that only carry out processing to keep, in accordance with law, a register that is intended to provide information to the public;
- organisations that only process manual data (unless the personal data have been prescribed by the ODPC as requiring registration); and
- organisations that are not established or conducted for profit and that are processing personal data related to their members and supporters and their activities.
Additionally, pursuant to SI No. 657 of 2007, the Irish Minister for Justice and Equality has specified that the following data controllers and data processors are not required to register (provided they do not fall within any of the categories noted above in respect of which no exemption may be claimed):

- a data controllers who only process employee data in the ordinary course of personnel administration and where the personal data are not processed other than where it is necessary to carry out such processing;
- b solicitors and barristers;
- c candidates for political office and elected representatives;
- d schools, colleges, universities and similar educational institutions;
- e normal commercial activity that by definition requires the processing of personal data (e.g., keeping details of customers and suppliers). This exemption does not include health professionals who process personal data relating to physical or mental health;
- f companies that process personal data relating to past or existing shareholders, directors or other officers of a company for the purpose of compliance with the Companies Acts;
- g data controllers who process personal data with a view to the publication of journalistic, literary or artistic material; and
- h data controllers or data processors who operate under an approved data protection code of practice.

If an exemption does apply, however, it is limited only to the extent to which personal data are processed within the scope of that exemption.

The ODPC is obliged not to accept an application for registration from a data controller who keeps ‘sensitive personal data’ unless the ODPC is of the opinion that appropriate safeguards for the protection of the privacy of the data subjects concerned are being, and will continue to be, provided by the controller.

Where the ODPC refuses an application for registration, it must notify the applicant in writing and specify the reasons for the refusal. An appeal against such a decision can be made to the circuit court.

### iii Technological innovation and privacy law

**Cloud computing**

The ODPC has issued guidance on issues that arise from processing data in the cloud. The data controller must be satisfied that the cloud service provider will only process the data in accordance with the data controller’s instructions. The data controller must also be satisfied that appropriate security measures have been taken by the cloud provider. These measures should cover continued access to the data by the data controller, prevention of unauthorised access to the data, adequate oversight of any sub-processors, procedures in the event of a data breach and the right to remove or transfer data. The data controller’s obligations in this respect can be satisfied by a detailed technical analysis incorporating an audit of the cloud provider or by third-party certification of the cloud provider to approved international standards.

A data controller must also assess the location of the data and must ensure that personal data are not transferred outside the EEA except in compliance with the DPA, for example, where the transfer is to an EU-approved country or pursuant to EU Model Contract Clauses or binding corporate rules (BCRs).
Finally, the data controller must ensure that a written contract is in place with the cloud provider.

**Biometrics**

The ODPC has published guidance on the use of biometric data both in the workplace and in schools, colleges and other educational institutions. The key issue in relation to biometric data is proportionality. The data controller must assess whether the biometric system is necessary and if there are less invasive alternatives available. Proportionality will depend on a number of factors, including the nature of the workplace or educational institution, the intended purpose of the system, efficiency and reliability. In the employment context, the ODPC’s stated position is that consent is not generally satisfactory, as it can be argued that it is not freely given in view of the typically imbalanced nature of the employer–employee relationship. Employers should seek to rely on the ‘legitimate interest’ ground for processing biometric data, but must ensure the right balance is struck between their interests and the employees’ rights. In the context of educational institutions, the ODPC recommends that consent is the only way of legitimising the processing of personal data. A clear and unambiguous right to opt out of the biometric system must be given. It is important that data subjects are made aware of the purpose of processing the biometric data.

The ODPC also highlights the importance of security in relation to biometric data, taking into account, in particular, the state of technological development, the cost of implementing security measures, the nature of the data being protected and the harm that might result through the unlawful processing of the data. The ODPC recommends that the personal data are deleted as soon as the employee or student permanently leaves.

The ODPC guidance recommends that employers and educational institutions conduct a privacy impact assessment prior to implementing a biometric system. This should take into account the need for such a system, the type of system required, the effect on data subjects and any less invasive options available.

iv Specific regulatory areas

**Health data**

The Data Protection (Access Modification) (Health) Regulations, 1989 provide that health data shall not be supplied to data subjects unless a health professional is first consulted and that access to the data is not likely to cause serious harm to the mental or physical health of the data subject.

The ODPC has published guidance in the area of research in the health sector. The ODPC is of the opinion that anonymisation of patient data is the optimal position for health research. Where this is not possible, or access to patient identifiable information is required, health research should be conducted on the basis of informed and freely given explicit consent.

The Health Identifiers Act 2014 was enacted in July 2014 (although it has only been partially commenced). It establishes a unique health identifier for each patient and provides that this shall be personal data for the purposes of the DPA. The Act provides for limitations on accessing and processing health identifiers and offences for non-compliance.11

---

Electronic communications marketing
Under the E-Privacy Regulations, using publicly available communications services to make any unsolicited calls or send unsolicited emails for the purpose of direct marketing is restricted.

Direct marketing by fax
A fax may not be used for direct marketing purposes with an individual who is not a customer, unless the individual in question has previously consented to receiving marketing communications by fax.

Direct marketing by phone
In summary, to contact an individual by phone for the purposes of direct marketing, the individual must have given his or her consent to receiving direct marketing calls (or to the receipt of communications to his or her mobile phone, as the case may be). In certain cases, it will be necessary to consult the National Directory Database prior to placing calls for marketing purposes.

Direct marketing by email or text message
To validly use these methods to direct market an individual, the individual concerned must have consented to the receipt of direct marketing communications via these methods.

The legislation provides for an exception whereby an existing customer may be taken to have consented on what is known as a ‘soft opt-in’ basis provided that certain requirements are met and that the service or product that is being marketed is either the same or very similar to the product previously sold to that person.

IV INTERNATIONAL DATA TRANSFER AND DATA LOCALISATION
Personal data may not be transferred outside the EEA unless one of the following applies:
  a  the transfer is authorised by law;
  b  consent to the transfer is given by the data subject;
  c  the transfer is necessary for the performance of a contract to which the data subject is party;
  d  the transfer is necessary to conclude a contract with someone other than the data subject, where it is in the data subject’s interests;
  e  the transfer is necessary for reasons of substantial public interest;
  f  the transfer is necessary for obtaining legal advice for legal proceedings;
  g  the transfer is necessary to prevent injury or damage to the data subject;
  h  the personal data to be transferred are an extract from a statutory public register established by law for public consultation; or
  i  the transfer is done through one of the mechanisms described in items (a), (b) or (c) below.

Even where one of the above elements exists, the ODPC retains the power to prohibit the transfer of personal data abroad to any country inside or outside the EEA.

In addition to the methods outlined above, the three methods by which Irish-based businesses typically transfer personal data outside the EEA are as follows:
Use of ‘model clauses’ between the data controller and the person or organisation to whom they intend to pass the information to abroad. These are contractual clauses approved by the European Commission and that assure an adequate level of protection for the personal data. They do not usually require the approval of the ODPC; however, it can approve transfers based on contractual clauses that do not directly conform to the European model clauses.

Transfer to a country that is on the European Commission ‘adequate standard of protection’ list, or US organisations that have agreed to be bound by the rules of the Privacy Shield agreement (essentially a streamlined version of EU data protection law).

A further method that is less frequent is using BCRs, whereby personal data can be transferred to other companies within a group and based abroad, as long as certain legally enforceable rules exist within the group whereby they must give the data an adequate level of protection. This method is less frequently used because of the expense and time involved in having these rules approved by the ODPC (which is a requirement to be able to rely on them).

V COMPANY POLICIES AND PRACTICES

While the DPA do not provide specifically for the appointment of a data protection officer, when registering with the ODPC, both data controllers and data processors must give details of a ‘compliance person’ who will supervise the application of the DPA within the organisation in relation to personal data that are collected.

Operators of websites are required to have privacy statements in place. This is required by both the DPA, which require data controllers to supply certain information to data subjects, and the E-Privacy Regulations, which require certain information to be supplied when information is stored or retrieved from a person’s terminal equipment, including the use of cookies. The privacy policy must contain the identity of the data controller, the purpose for which personal data will be processed and the parties to whom the data will be disclosed. Data subjects must also be informed of their rights of access, rectification and erasure under the DPA. The ODPC also recommends including information such as the retention period and complaint resolution mechanism. The ODPC recommends placing a link to the privacy statement in a reasonably obvious position on each page of websites.

Although not strictly required, it is recommended that data controllers implement a security policy. The ODPC recommends that this include data collection and retention, access control, a ‘movers, leavers and joiners’ policy and an incident response plan.

VI DISCOVERY AND DISCLOSURE

Where data are sought for use in civil proceedings in a foreign country, Irish companies may be compelled under a subpoena from an Irish court to provide them. This happens frequently between EU countries, but it is also possible for a request from outside the EU to succeed.

In relation to requests from foreign law enforcement agencies, there is a legal framework in place that allows for the law enforcement agencies of foreign signatories of certain Hague Conventions to seek the disclosure of data held by Irish companies by the Irish police, who then issue a warrant for it. Where the request is made by the law enforcement agencies of countries that are not signatories, this is determined by the Department of Justice and
Equality on a case-by-case basis. Generally, where proper undertakings are given by the agency making the request, it will be granted and Irish companies will be compelled to disclose the data.

Part 3 of the Criminal Justice (Mutual Assistance) Act 2008 provides for various forms of mutual legal assistance to foreign law enforcement authorities. Part 3 relates to requests for mutual assistance between Ireland and other EU Member States for cooperation in the policing of telecommunications messages for the purposes of criminal investigations. The Minister for Justice can also now request that tapping of communications be undertaken in an EU Member State for an Irish-based criminal investigation and also outlines how requests from other EU countries to Ireland for such interceptions should be processed.

The ODPC has not, as yet, issued official guidance in relation to foreign e-discovery requests or requests for disclosure from foreign law enforcement agencies. However, it is clear from statements by the government expressed prior to the most recent decision in the Microsoft Warrant case that the government advocates the use of existing mutual legal assistance treaties as a means of providing assistance in legal cases or law enforcement investigations.

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

The DPA confer specific rights on the ODPC and explicitly state that the ODPC shall be the supervisory authority in Ireland for the purpose of the Directive. The ODPC is responsible for ensuring that individuals’ data protection rights are respected and that those who are in control of or who process personal data carry out their responsibilities under the DPA.

Powers of the ODPC

Investigations

The ODPC must investigate any complaints that it receives from individuals in relation to the treatment of their personal data unless it considers them to be ‘frivolous or vexatious’. The ODPC may also carry out investigations of its own accord. In practice, these usually take the form of scheduled privacy audits. However, it should be noted that the ODPC is not prevented from conducting ‘dawn raid’ types of audits if it decides to do so.

Power to obtain information

The ODPC has the power to require any person to provide it with whatever information it needs to carry out its functions. In carrying out this power in practice, the ODPC usually issues the person with an information notice in writing. It is an offence to fail to comply with such an information notice (without reasonable excuse), although there is a right to appeal any requirement specified in an information notice to the circuit court.

Power to enforce compliance with the DPA

The ODPC may require a data controller or data processor to take whatever steps it considers appropriate to comply with the terms of the DPA. In practice, this may involve blocking personal data from use for certain purposes, or erasing, correcting or supplementing the
personal data. This power is exercised by the ODPC issuing an enforcement notice. It is an offence to fail to comply with an enforcement notice (although there is also a right of appeal against such a notice as there is for an information notice referred to above).

**Power to prohibit overseas transfer of personal data**

Under Section 11 of the DPA, the ODPC may prohibit the transfer of personal data from Ireland to an area outside the EEA. In exercising this power, the ODPC must have regard to the need to facilitate international transfers of information.

**Powers of ‘authorised officers’**

The ODPC has the power to nominate an authorised officer to enter and examine the premises of a data controller or data processor, to enable the ODPC to carry out its functions. An authorised officer has a number of powers, such as the power to enter the premises and inspect any data equipment there; to require the data controller or data processor to assist him or her in obtaining access to personal data; and to inspect and copy any information.

**Enforcement**

The ODPC may bring summary legal proceedings for an offence under the DPA. However, in contrast to the position in certain other jurisdictions such as the United Kingdom, the ODPC does not have the power to impose fixed monetary penalties.

**Sanctions**

While most of the penalties for offences under the DPA are civil in nature, breaches of data protection can also lead to criminal penalties. Summary legal proceedings for an offence under the DPA may be brought and prosecuted by the ODPC. Under the DPA, the maximum fine on summary conviction of such an offence is set at €3,000. On conviction on indictment (such a conviction in Ireland is usually reserved for more serious crime), the maximum penalty is a fine of €100,000.

The E-Privacy Regulations specify the sanctions for breaches of electronic marketing restrictions, which on summary conviction are a fine of up to €5,000 (per communication) or, on conviction on indictment, maximum fines ranging from €50,000 for a natural person to €250,000 for a body corporate.

The ODPC exercises its powers of enforcement on a regular basis, including through conducting inspections of organisations. During the course of 2015, 51 audits and inspections were carried out and four entities were prosecuted for a total of 24 offences.

**Recent enforcement cases**

**Excessive use of CCTV**

In 2015, the ODPC addressed a number of cases where companies were using CCTV systems in a manner incompatible with the DPA and the ODPC’s guidance. While no fines were imposed, the ODPC issued a number of case studies on the topic.
Marketing offences

A number of companies were prosecuted in 2015 for making unsolicited marketing calls and communications. In one case, a fine of €1,000 was imposed. Orders to make charitable donations ranging from €1,000 and up to €35,000 were also made (this approach is sometimes applied by courts as an alternative to levying a fine).

iii Private litigation

The DPA provide a statutory duty of care on the part of data controllers and processors in favour of data subjects. Thus, an individual can sue under the law of torts for a breach of any obligations under the DPA. The High Court has held that it is necessary for a data subject to show harm has resulted from a breach before any right to compensation will arise under this section.12

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

The DPA apply to data controllers in respect of the processing of personal data only if:

a the data controller is established in Ireland and the data are processed in the context of that establishment; or

b the data controller is established neither in Ireland nor in any other state that is a contracting party to the EEA Agreement, but makes use of equipment in Ireland for processing the data otherwise than for the purpose of transit through the territory of Ireland. Such a data controller must, without prejudice to any legal proceedings that could be commenced against the data controller, designate a representative established in Ireland.

Each of the following shall be treated as established in Ireland:

a an individual who is normally resident in Ireland;

b a body incorporated under the laws of Ireland;

c a partnership or other unincorporated association formed under the laws of Ireland; and

d a person who does not fall within any of the above, but who maintains in Ireland an office, branch or agency through which he or she carries on any activity, or a regular practice.

IX CYBERSECURITY AND DATA BREACHES

The ODPC has published the Personal Data Security Breach Code of Practice (Code), which contains specific data security breach guidelines. This Code is non-binding in nature and does not apply to providers of publicly available electronic communications services in public communications networks in Ireland, which are subject to a mandatory reporting obligation under the E-Privacy Regulations.

The following guidelines are provided for in the Code:

a when a data breach occurs, the data controller should immediately consider whether to inform those who will be or have been impacted by the breach;

12 Collins v. FBD Insurance plc [2013] IEHC 137.
if a breach is caused by a data processor, he or she should report it to the data controller as soon as he or she becomes aware of it;

c if the personal data was protected by technological measures (such as encryption) to such an extent that it would be unintelligible to any person who is not authorised to access it, then the data controller may decide that there is no risk to the personal data (and so no notification to the data subject is necessary);

d any incident that has put personal data at risk should be reported to the ODPC as soon as the data controller becomes aware of it. There are some limited exceptions to this provided for in the Code; for example, this is not required where:

• it affects fewer than 100 data subjects;
• the full facts of the incident have been reported without delay to those affected; and
• the breach does not involve sensitive personal data or personal data of a financial nature; and

e if the data controller is unclear about whether to report the incident, the Code advises that the incident should be reported to the ODPC. The Code advises that the controller should make contact with the ODPC within two working days of the incident occurring.

Once the ODPC is made aware of the circumstances surrounding a breach or a possible breach, it will decide whether a detailed report or an investigation (or both) is required.

Regarding cybersecurity, the government is in the process of implementing the National Cyber Security Strategy 2015–2017, which established the National Cyber Security Centre (NCSC) within the Department of Communications, Energy and Natural Resources and outlines the government’s plan to address the risks posed by cybercrime to the digital economy and society. The objectives include:

a improving the resilience and robustness of the critical information infrastructure in crucial economic sectors;

b engaging with international partners to ensure that cyberspace remains open, secure, unitary and free;

c raising awareness of the responsibilities of businesses and individuals;

d ensuring that Ireland has a comprehensive and flexible legal and regulatory framework in place to combat cybercrime; and

e building capacity to engage in the emergency management of cyber incidents.

The NCSC aims to build on the work of the Computer Security Incident Response Team, which was established in 2011. The NCSC also intends to introduce legislation to transpose the EU Network and Information Security Directive (which was approved in 2016), the Budapest Convention on Cybercrime and Directive 2013/40/EU on attacks against information systems.

In September 2016, the Central Bank of Ireland, the regulator for financial institutions, published Cross Industry Guidance in respect of Information Technology and Cybersecurity, which relates to IT governance and risk management by regulated financial institutions in Ireland.
X OUTLOOK

The main feature of the short to mid-term Irish data protection landscape is the coming into effect of the General Data Protection Regulation (GDPR) in May 2018. With the final text of the GDPR now published, businesses are starting to familiarise themselves with the new regime that the GDPR will bring about. We are already seeing controllers and processors alike looking to implement aspects of the GDPR, notably privacy by design in new product and service offerings that they plan to roll out between now and May 2018.

The next phase of proceedings regarding data transfers has already started in the Irish courts. The ODPC is seeking a ruling from the CJEU on whether, following the Schrems decision, the transfer of data to the United States based on model clauses is permissible. It is expected that the Irish courts’ decision as to whether to make the referral will be issued in 2017.

In its most recent Annual Report, the ODPC lists its next priorities as including the expansion of its capacity and capability, and working closely with all stakeholders, and particularly with the Article 29 Working Party, towards the implementation of the GDPR.
I  OVERVIEW

In Japan, the Act on the Protection of Personal Information (APPI) primarily handles the protection of data privacy issues. The APPI was drastically amended in 2016 and has been in full force since 30 May 2017. Prior to the amendment, the APPI was applied solely to business operators that have used any personal information database containing details of more than 5,000 persons on any day in the past six months but this requirement was eliminated by the amendment. Under the amended APPI, the Personal Information Protection Commission (PPC) was established as an independent agency whose duties include protecting the rights and interests of individuals while promoting proper and effective use of personal information. Under the amended APPI, the legal framework has been drastically changed and the PPC has primary responsibility for personal information protection policy in Japan. Prior to the amendment, as of July 2015, 39 guidelines for 27 sectors regarding personal information protection were issued by government agencies, including the Ministry of Health, Labour and Welfare, the Japan Financial Services Agency, and the Ministry of Economy, Trade and Industry. Under the amended IPPI, however, the guidelines (the APPI Guidelines) that prescribe in detail the interpretations and practices of the APPI are principally provided by the PPC, with a limited number of special guidelines provided to specific sectors (such as medical and financial ones) by the PPC and the relevant ministries.

---

1 Tomoki Ishiara is counsel at Sidley Austin Nishikawa Foreign Law Joint Enterprise.
II THE YEAR IN REVIEW

i Background of the amendment to the APPI: Policy Outline of the Institutional Revision for Use of Personal Data (the Policy Outline), and the amendment to the APPI

On 24 June 2014, the government⁹ published the Policy Outline,¹⁰ showing the government’s direction on the measures to be taken to amend the APPI and the other personal information protection-related laws. The revision bill of the APPI passed the Diet on 3 September 2015 and the amended APPI has been in full force since 30 May 2017. The main changes introduced by the amendment to the APPI are set out below.

Development of a third-party authority system

The government has established an independent agency to serve as a data protection authority to operate ordinances and self-regulation in the private sector to promote the use of personal data. The primary amendments to the previous legal framework are as follows:

a the government has established the structure of the third-party authority ensuring international consistency, so that legal requirements and self-regulation in the private sector are effectively enforced;

b the government has restructured the Specific Personal Information Protection Commission prescribed in the Number Use Act¹² to set up the PPC, the new authority mentioned at (a), for the purpose of promoting a balance between the protection of personal data and effective use of personal data; and

c the third-party authority has the following functions and powers:

• formulation and promotion of basic policy for personal information protection;
• supervision;
• mediation of complaints;
• assessment of specific personal information protection;
• public relations and promotion;
• accreditation of private organisations that process complaints about business operators handling personal information and provide necessary information to such business operators, based on the amended Act on the Protection of Personal Information;
• survey and research the operations stated above at (c); and
• cooperation with data protection authorities in foreign states.¹³

---

⁹ Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society.
¹¹ The European Commission pointed out the lack of a data protection authority in the Japanese system in its report: Korfe, Brown, et al., ‘Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments’ (20 January 2010).
¹² Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedure (Act No. 27 of 2013). See Section II.ii.
¹³ Article 61 APPI.
Actions for globalisation
If businesses handling personal data are planning to provide personal data (including personal data provided by overseas businesses and others) to overseas businesses, they have to obtain consent to the transfer from the principal\(^{14}\) except where:

\(\begin{align*}
\text{a} & \text{ no consent is necessary in accordance with the following exceptions to Article 23(1):} \\
& \text{• cases based on laws and regulations;} \\
& \text{• cases in which there is a need to protect a human life, body or fortune, and when it is difficult to obtain a principal’s consent;} \\
& \text{• cases in which there is a special need to enhance public hygiene or promote fostering healthy children, and when it is difficult to obtain a principal’s consent; and} \\
& \text{• cases in which there is a need to cooperate with a central government organisation or a local government, or a person entrusted by them acting in matters prescribed by laws and regulations,}\(^\text{15}\) and when there is a possibility that obtaining a principal’s consent would interfere with the execution of these duties; }
\end{align*}\)

\(\begin{align*}
\text{b} & \text{ the overseas businesses establish a system conforming to operating standards prescribed by the PPC rules for overseas businesses to deal with personal information in a manner equivalent to that of a business operator handling personal data pursuant to the provisions of the APPI; and} \\
\text{c} & \text{ the foreign countries in which the overseas businesses are conducted are prescribed by the PPC rules as having established a personal information protection system with standards equivalent to those in Japan regarding the protection of an individual's rights and interests.}
\end{align*}\)

Framework for promoting the use of personal data (big data issues)
The use of personal data is expected to create innovation with the multidisciplinary utilisation of diverse and vast amounts of data, thereby creating new businesses. However, the system under the previous APPI required consent from principals to use their personal data for purposes other than those specified. Accordingly, providing personal data to third parties was cumbersome for businesses, and created a barrier to the use of personal data, especially launching new business using big data. Under the amended APPI, a business operator handling personal information may produce anonymously processed information (limited to information constituting anonymously processed information databases, etc.) and process personal information in accordance with standards prescribed by the PPC rules such that it is impossible to identify a specific individual from, or de-anonymise, the personal information used for the production.\(^\text{16}\) This amendment allows various businesses to share with other businesses the personal data maintained by them, and so develop or foster new business or innovation.

Sensitive personal information
The previous APPI did not define ‘sensitive personal information’; however, the amended APPI has defined information regarding an individual’s race, creed, social status, criminal record and

\(^{14}\) Article 24 APPI.
\(^{15}\) Article 23 APPI.
\(^{16}\) Article 36(1) APPI.
past record as ‘special-care-required personal information’ (sensitive personal information), along with any other information that may be the focus of social discrimination. Also, there was no provision that specifically addressed consent requirements for sensitive personal information in the previous APPI; instead these were regulated by a number of guidelines issued by government ministries. The amended APPI, however, explicitly requires that a business operator handling personal information obtain prior consent to acquire sensitive personal information, with certain exceptions.

In addition, the opt-out exception provided under Article 23 does not apply to sensitive personal information and consent to provide such information to third parties is required. The Policy Outline also mentions that in view of the actual use of personal information, including sensitive information, and the purpose of the current law, the government will lay down regulations regarding the handling of personal information, such as providing exceptions where required by laws and ordinances and for the protection of human life, health or assets, as well as enabling personal information to be obtained and handled with the consent of the persons concerned.

Enhancement of the protection of personal information: tractability of obtained personal information

The amended revised APPI:

a imposes obligations on business operators handling personal information to make and keep accurate records for a certain period when they provide third parties with personal information;

b imposes obligations on business operators handling personal information to verify third parties’ names and how they obtained personal information upon receipt of personal information from those third parties; and

c establishes criminal liability for providing or stealing personal information with a view to making illegal profits.

ii Social security numbers

The bill on the use of numbers to identify specific individuals in administrative procedures (the Number Use Act, also called the Social Security and Tax Number Act) was enacted on 13 May 2013, and provides for the implementation of a national numbering system for social security and taxation purposes. The government will adopt the social security and tax number system to enhance social security for people who truly need it; to achieve the fair distribution of burdens such as income tax payments; and to develop efficient administration. The former independent supervisory authority called the Specific Personal Information Protection Commission was transformed into the PPC, which was established on 1 January 2016 to handle matters with respect to both the Number Use Act and the

17 Article 1(3) APPI.
18 Article 17(2) APPI.
19 Article 23(2) APPI.
20 Article 25 APPI.
21 Article 26 APPI.
22 Article 83 APPI.
23 The revision bill of the Number Use Act was passed on 3 September 2015. The purpose of this revision was to provide further uses for the numbering system (e.g., management of personal medical history).
amended APPI. This authority consists of one chair and eight commission members. The chair and commissioners were appointed by Japan’s prime minister and confirmed by the National Diet. The numbering system fully came into effect on 1 January 2016. Unlike other national ID numbering systems, Japan has not set up a centralised database for the numbers because of concerns about data breaches and privacy.

iii  Online direct marketing

Under the Act on Regulation of Transmission of Specified Electronic Mail and the Act on Specified Commercial Transactions, businesses are generally required to provide recipients with an opt-in mechanism, namely to obtain prior consent from each recipient for any marketing messages sent by electronic means. A violation of the opt-in obligation may result in imprisonment, a fine, or both.

iv  Reciprocal adequacy decision

On 17 July 2018, Japan released a press release announcing Japan and the European Union (EU) have agreed on reciprocal adequacy of their respective data protection systems. Japan and the EU have long discussed and agreed on reciprocal adequacy on the condition that Japan would implement guidelines (without revising the APPI) to supplement insufficient protections from the EU perspective as follows.

\[
\begin{align*}
  a & \quad \text{Information on trade union membership or an individual’s sexual orientation shall be regarded as sensitive information in Japan as well as in the EU.} \\
  b & \quad \text{Personal data that will be deleted within six months shall be protected as personal data.} \\
  c & \quad \text{The purpose of use of personal information provided by a third party is limited to that originally set by the third party.} \\
  d & \quad \text{Japan shall ensure the same level of protection as in Japan if personal information coming from the EU is transferred from Japan to non-EU countries.} \\
  e & \quad \text{For the anonymisation of personal information coming from the EU, the complete deletion of a method of re-identification would be required.}
\end{align*}
\]

III  REGULATORY FRAMEWORK

i  Privacy and data protection legislation and standards

Definitions

**Personal information**

The amended APPI clarifies the scope of ‘personal information’ as follows:

---

27  Under the APPI, by definition, this information is not defined as sensitive information.
28  Article 2(7) APPI does not grant the right to correct, add and delete etc. to personal information that would be deleted within six months.
29  Article 36(2) APPI does not require a personal information handling business operator to delete the information on a method of anonymisation but take actions for security control such information.
a information about a living person that can identify him or her by name, date of birth or other description contained in the information (including information that will allow easy reference to other information that will enable the identification of the specific individual);\(^{30}\) or

b information about a living person that contains an individual identification code, which means any character, letter, number, symbol or other codes designated by Cabinet Order,\(^{31}\) falling under any of the following items:

- those able to identify a specific individual that are a character, letter, number, symbol or other codes into which a bodily or partial feature of the specific individual has been converted to be provided for use by computers; and
- those characters, letters, numbers, symbols or other codes assigned in relation to the use of services provided to an individual, or to the purchase of goods sold to an individual, or that are stated or electromagnetically recorded in a card or other document issued to an individual so as to be able to identify a specific user or purchaser, or recipient of issuance by having made the said codes differently assigned or stated or recoded for the said user or purchaser, or recipient of issuance.\(^{32}\)

**Personal information database**

A ‘personal information database’\(^{33}\) is an assembly of information including:

a information systematically arranged in such a way that specific personal information can be retrieved by a computer; or

b in addition, 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.

**Business operator handling personal information**

A ‘business operator handling personal information’\(^{34}\) is a business operator using a personal information database, etc. for its business.\(^{35}\) However, the following entities shall be excluded:

a state organs;

b local governments;

c incorporated administrative agencies, etc.;\(^{36}\) and

d local incorporated administrative institutions.\(^{37}\)

---

30 Article 2(1)(i) APPI.
31 Article 2(1)(ii), Article 2(2) APPI.
32 For example, according to the Cabinet Order, the information on sequences of bases of DNA, fingerprints, facial recognition (Article 2(2)(i)) and the information on driver licence, passport and insurance policy number (Article 2(2)(ii)) are regarded as an individual identification code.
33 Article 2(4) APPI.
34 Article 2(5) APPI.
35 As mentioned in Section I, the amended APPI applies to business operators that use any personal information database, regardless of the number of principals of personal information. Prior to the amendment, the APPI was applied solely to any personal information database containing details of more than 5,000 persons on any day in the past six months. See footnote 3.
36 Meaning independent administrative agencies as provided in Paragraph (1) of Article 2 of the Act on the Protection of Personal Information Held by Incorporated Administrative Agencies, etc. (Act No. 59 of 2003).
37 Meaning local incorporated administrative agencies as provided in Paragraph (1) of Article 2 of the Local Incorporated Administrative Agencies Law (Act No. 118 of 2003).
Personal data

‘Personal data’ comprises personal information constituting a personal information database, etc. (when personal information such as names and addresses is compiled as a database, it is personal data in terms of the APPI).

Sensitive personal information

The previous APPI did not have a definition of ‘sensitive personal information’. However, for example, the Japan Financial Services Agency’s Guidelines for Personal Information Protection in the Financial Field (the JFSA Guidelines) have defined information related to political opinion, religious belief (religion, philosophy, creed), participation in a trade union, race, nationality, family origin, legal domicile, medical care, sexual life and criminal record as sensitive information. Furthermore, the JFSA Guidelines prohibit the collection, use or provision to a third party of sensitive information, although some exceptions exist. Following these practices, the amended APPI has explicitly provided a definition of ‘sensitive personal information’ and its special treatment (see Section II.i).

ii General obligations for data handlers

Purpose of use

Pursuant to Article 15(1) APPI, a business operator handling personal information must as far as possible specify the purpose of that use. In this regard, the Basic Policy on the Protection of Personal Information (Basic Policy) (Cabinet Decision of 2 April 2004) prescribes as follows:

To maintain society’s trust of business activities, it is important for businesses to announce their appropriate initiatives for complaint processing and not using personal information for multiple uses through the formulation and announcement of their policies (so-called privacy policies or privacy statements, etc.) and philosophies on the promotion of the personal information protection. It is also important for businesses to externally explain, in advance and in an easy-to-understand manner, their procedures relating to the handling of personal information, such as notification and announcement of the purpose of use and disclosure, etc., as well as comply with the relevant laws and ordinances.

The government formulated the Basic Policy based on Article 7, Paragraph 1 APPI. To provide for the complete protection of personal information, the Basic Policy shows the orientation of measures to be taken by local public bodies and other organisations, such as businesses that handle personal information, as well as the basic direction concerning the promotion of measures for the protection of personal information and the establishment of measures to be taken by the state. The Basic Policy requires a wide range of government and private entities to take specific measures for the protection of personal information.

In this respect, under the previous APPI, a business operator handling personal information could not change the use of personal information ‘beyond a reasonable extent’. The purpose of use after the change therefore had to be duly related to that before the change.

---

38 Article 2(6) APPI.
40 Article 6(1) of the JFSA Guidelines.
41 Article 6(1)1–8 of the JFSA Guidelines.
The amended APPI has slightly expanded the scope of altering the purpose of use to enable flexible operations by prohibiting alteration of the utilisation purpose ‘beyond the scope recognised reasonably relevant to the pre-altered utilisation purpose’.\(^4\) In addition, a business operator handling personal information must not handle personal information about a person beyond the scope necessary for the achievement of the purpose of use, without obtaining the prior consent of the person.\(^4\)

**Proper acquisition of personal information and notification of purpose**

A business operator handling personal information shall not acquire personal information by deception or other wrongful means.\(^4\)

Having acquired personal information, a business operator handling personal information must also promptly notify the data subject of the purpose of use of that information or publicly announce the purpose of use, except in cases in which the purpose of use has already been publicly announced.\(^4\)

**Maintenance of the accuracy of data and supervision of employees or outsourcing contractors**

A business operator handling personal information must endeavour to keep any personal data it holds accurate and up to date within the scope necessary for the achievement of the purpose of use. Under the amended APPI,\(^4\) a business operator handling personal information also must endeavour to delete personal data without delay when it becomes unnecessary.

In addition, when a business operator handling personal information has an employee handle personal data, it must exercise necessary and appropriate supervision over the employee to ensure the secure control of the personal data.\(^4\)

When a business operator handling personal information entrusts another individual or business operator with the handling of personal data in whole or in part, it shall also exercise necessary and appropriate supervision over the outsourcing contractor to ensure the secure control of the entrusted personal data.\(^4\)

**Restrictions on provision to a third party**

In general, a business operator handling personal information must not provide personal data to a third party without obtaining the prior consent of the data subject.\(^4\)

\(^{4}\) Article 15(2) APPI.
\(^{43}\) Article 16(1) APPI.
\(^{44}\) Article 17 APPI.
\(^{45}\) Article 18(1) APPI.
\(^{46}\) Article 19 APPI.
\(^{47}\) Article 21 APPI. For example, during training sessions and monitoring, whether employees comply with internal rules regarding personal information protection.
\(^{48}\) Article 22 APPI. The APPI Guidelines point out: (1) a business operator handling personal information has to prepare rules on the specific handling of personal data to avoid unlawful disclosure and maintain the security of personal data; and (2) a business operator handling personal information has to take systemic security measures (e.g., coordinate an organisation’s operations with regard to the rules on the handling of personal data, implement measures to confirm the treatment status of personal data, arrange a system responding to unlawful disclosure of personal data and review the implementation or improvement of security measures).
\(^{49}\) Article 23(1) APPI.
The principal exceptions to this restriction are where:

a. the provision of personal data is required by laws and regulations;\(^{50}\)

b. a business operator handling personal information agrees, at the request of the subject, to discontinue providing such personal data as will lead to the identification of that person, and where the business operator, in advance, notifies the PPC and the person of the following or makes this information readily available to the person in accordance with the rules set by the PPC:\(^{51}\)

- the fact that the provision to a third party is the purpose of use;
- which items of personal data will be provided to a third party;
- the method of provision to a third party;
- the fact that the provision of such personal data as might lead to the identification of the person to a third party will be discontinued at the request of the person; and
- the method of receiving the request of the person.

c. a business operator handling personal information outsources the handling of personal data (e.g., to service providers), in whole or in part, to a third party within the scope necessary for the achievement of the purpose of use;\(^{52}\)

d. personal information is provided as a result of the takeover of business in a merger or other similar transaction;\(^{53}\) and

e. personal data is used jointly between specific individuals or entities and where the following are notified in advance to the person or put in a readily accessible condition for the person:

- the facts;
- the items of the personal data used jointly;
- the scope of the joint users;
- the purpose for which the personal data is used by them; and
- the name of the individual or entity responsible for the management of the personal data concerned.\(^{54}\)

**Public announcement of matters concerning retained personal data**

Pursuant to Article 24(1) APPI, a business operator handling personal information must put the name of the business operator handling personal information and the purpose of use of all retained personal data in an accessible condition for the person concerned (this condition

---

50 Article 23(1)(i) APPI. The APPI Guidelines mention the following cases:

a. response to a criminal investigation in accordance with Article 197(2) of the Criminal Procedure Law;
b. response to an investigation based upon a warrant issued by the court in accordance with Article 218 of the Criminal Procedure Law; and
c. response to an inspection conducted by the tax authority.

51 Article 23(2) APPI.

52 Article 23(5)(i) APPI.

53 Article 23(5)(ii) APPI.

54 Article 23(5)(iii) APPI.
of accessibility includes cases in which a response is made without delay upon the request of the person), the procedures for responding to a request for disclosure, correction and cessation of the retention of the personal data.\(^{55}\)

**Correction**

When a business operator handling personal information is requested by a person to correct, add or delete such retained personal data as may lead to the identification of the person on the ground that the retained personal data are incorrect, the business operator must make an investigation without delay within the scope necessary for the achievement of the purpose of use and, on the basis of the results, correct, add or delete the retained personal data, except in cases where special procedures are prescribed by any other laws and regulations for such correction, addition or deletion.\(^{56}\)

### IV INTERNATIONAL DATA TRANSFER AND DATA LOCALISATION

**i Extraterritorial application of the APPI**

It was generally considered that when an entity handling personal information in Japan obtains personal information from business operators outside Japan or assigns personal information to business operators outside Japan, the APPI would be applicable to the entity handling personal information in Japan. In accordance with this accepted understanding, the amended APPI explicitly provides that the APPI applies to a business operator located outside Japan under certain circumstances.

The provisions of Article 15, Article 16, Article 18 (excluding Paragraph (2)), Articles 19 to 25, Articles 27 to 36, Article 41, Article 42 Paragraph (1), Article 43 and Article 76 apply in those cases where, in relation to provision of a good or service to a person in Japan, a business operator handling personal information has acquired personal information relating to that person and handles the personal information or anonymously processed information produced using the said personal information in a foreign country.\(^{57}\)

**ii International data transfers**

With some exceptions prescribed in the APPI (see Section III.ii, ‘Restrictions on provision to a third party’), prior consent is required for the transfer of personal information to a third party.\(^{58}\) However, there was no specific provision regarding international data transfers in the previous APPI. To deal with the globalisation of data transfers, the amended APPI requires the consent of the principal to international transfers of personal data except in the following cases:\(^{59}\)

\(a\) international personal data transfer to a third party (in a foreign country) that has established a system conforming to the standards set by the PPC rules\(^{60}\) (i.e., proper

---

55 The APPI Guidelines provide examples of what corresponds to such an accessible condition for the person, such as posting on the website, distributing brochures, replying without delay to a request by the person and providing the email address for enquiries in online electronic commerce.

56 Article 29(1) APPI.

57 Article 75 APPI.

58 Article 23(1) APPI.

59 Article 24 APPI.

60 Article 11 Rules of the PPC.
and reasonable measures taken in accordance with the provisions of the APPI or accreditation as a receiver of personal data according to international standards on the protection of personal information, such as being certified under the Asia-Pacific Economic Cooperation Cross-Border Privacy Rules) for operating in a manner equivalent to that of a business operator handling personal data; and international personal data transfer to a third party in a foreign country that is considered, according to the rules of the PPC, to have established a personal information protection system with standards equivalent to those in Japan regarding the protection of an individual’s rights and interests.61

V COMPANY POLICIES AND PRACTICES

i Security control measures

A business operator handling personal information must take necessary and proper measures for the prevention of leakage, loss or damage of the personal data.62 Control measures may be systemic, human, physical or technical. Examples of these are listed below.

Systemic security control measures63

a Preparing the organisation’s structure to take security control measures for personal data;
b preparing the regulations and procedure manuals that provide security control measures for personal data, and operating in accordance with the regulations and procedure manuals;
c preparing the means by which the status of handling personal data can be looked through;
d assessing, reviewing and improving the security control measures for personal data; and
e responding to data security incidents or violations.

Human security control measures64

a Concluding a non-disclosure agreement with workers when signing the employment contract and concluding a non-disclosure agreement between an entruster and trustee in the entrustment contract, etc. (including the contract of supply of a temporary labourer); and

b familiarising workers with internal regulations and procedures through education and training.

61 At the time of writing, the PPC has not yet designated any country as having standards equivalent to those in Japan regarding the protection of personal information but the PPC has announced that it will designate member countries of the EU as qualified ones. See Section II.iv.

62 Article 20 APPI.

63 8-3 (Systemic Security Control Measures) of the APPI Guidelines, p. 88.

64 8-4 (Human Security Control Measures) and 3-3-3 (Supervision of Employees) of the APPI Guidelines, pp. 92, 41.
**Physical security control measures**

- Implementing controls on entering and leaving a building or room where appropriate;
- preventing theft, etc.; and
- physically protecting equipment and devices.

**Technical security control measures**

- Identification and authentication for access to personal data;
- control of access to personal data;
- management of the authority to access personal data;
- recording access to personal data;
- countermeasures preventing unauthorised software on an information system handling personal data;
- measures when transferring and transmitting personal data;
- measures when confirming the operation of information systems handling personal data; and
- monitoring information systems that handle personal data.

**VI DISCOVERY AND DISCLOSURE**

**i E-discovery**

Japan does not have an e-discovery system equivalent to that in the United States. Electronic data that include personal information can be subjected to a judicial order of disclosure by a Japanese court during litigation.

**ii Disclosure**

When a business operator handling personal information is requested by a person to disclose such retained personal data as may lead to the identification of the person, the business operator must disclose the retained personal data without delay by a method prescribed by a Cabinet Order. However, in the following circumstances, the business operator may keep all or part of the retained personal data undisclosed where disclosure:

- is likely to harm the life, person, property, or other rights or interests of the person or a third party;
- is likely to seriously impede the proper execution of the business of the business operator handling the personal information; or
- violates other laws and regulations.

---

65 8-5 (Physical Security Control Measures) of the APPI Guidelines, p. 93.
66 8-6 (Technical Security Control Measures) of the APPI Guidelines, p. 96.
67 The method specified by a Cabinet Order under Article 28(2) APPI shall be the provision of documents (or ‘the method agreed upon by the person requesting disclosure, if any’). Alternatively, according to the APPI Guidelines, if the person who made a request for disclosure did not specify a method or make any specific objections, then they may be deemed to have agreed to whatever method the disclosing entity employs.
68 Article 28(2) APPI.
VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement and sanctions

Enforcement agencies
Prior to the amendment, the enforcement agencies in data protection matters were the Consumer Affairs Agency, and ministries and agencies concerned with jurisdiction over the business of the relevant entities. Under the amended APPI, the PPC is the sole enforcement authority and it may transfer its authorities to request for report and to inspect to ministries and agencies if necessary for effective recommendations and orders under Article 42.69

Main penalties70
A business operator that violates orders issued under Paragraphs 2 or 3 of Article 42 (recommendations and orders by the PPC in the event of a data security breach) shall be sentenced to imprisonment with forced labour of not more than six months or to a fine of not more than ¥300,000.71

A business operator that does not make a report72 as required by Articles 40 or 56 or that has made a false report shall be sentenced to a fine of not more than ¥300,000.73

ii Recent enforcement cases

Information breach at a computer company
An outsourcing contractor of a computer company had their customer information acquired by a criminal following an illegal intrusion into the company’s network system. In May 2011, the Ministry of Economy, Trade and Industry promulgated an administrative guidance requesting that the computer company reform its security control measures, supervision of outsourcing contractors, and training for outsourcing contractors and employees (in respect of violation of the duty regarding supervision of an outsourcing contractor under Article 22 APPI).74

Information breach at a mobile phone company
The email addresses of a mobile phone company were reset and email addresses of the customers and the mail texts were disclosed to third parties. In January 2012, the Ministry of Internal Affairs and Communications (MIC) promulgated an administrative guidance requesting

69 Article 44 APPI.
70 The Unfair Competition Prevention Act (Act No. 47 of 1993) prohibits certain acts (unfair competition), including an act to acquire a trade secret from the holder by theft, fraud or other wrongful methods; and an act to use or disclose the trade secret so acquired. For the prevention of unfair competition, the Act provides measures, such as injunctions, claims for damages and penal provisions (imprisonment for a term not exceeding 10 years or a fine in an amount not exceeding ¥20 million. In the case of a juridical person, a fine not exceeding ¥1 billion (in certain cases the fine is not to exceed ¥500 million) may be imposed (Articles 21 and 22)).
71 Article 84 APPI.
72 The PPC may have a business operator handling personal information make a report on the handling of personal information to the extent necessary for fulfilling the duties of a business operator (Articles 40 and 56 APPI).
73 Article 85 APPI.
74 3-3-4 of the APPI Guidelines, p.42.
that the mobile phone company take the necessary measures to prevent a recurrence and to report the result to the Ministry (in respect of violation of the duty regarding security control measures under Article 20 APPI).76

Information theft from mobile phone companies

The manager and employees of an outsourcing contractor of three mobile phone companies acquired customer information from the mobile phone companies unlawfully through their customer information management system and disclosed the customer information to a third party. In November 2012, the MIC introduced an administrative guidance requesting that the mobile phone companies reform their security control measures, supervision of outsourcing contractors, and training for outsourcing contractors and employees (in respect of violation of the duty regarding security control measures under Article 20 APPI and Article 11 of the MIC Guideline on Protection of Personal Information in Telecommunications.77 There was also found to be a violation of the duty regarding the supervision of outsourcing contractors under Article 22 APPI and Article 12 of the above-mentioned MIC Guideline).78

Information theft from a mobile phone company

In July 2012, a former store manager of an agent company of a mobile phone company was arrested for disclosing customer information of the mobile phone company to a research company (in respect of violation of the Unfair Competition Prevention Act). The Nagoya District Court in November 2012 gave the defendant a sentence of one year and eight months’ imprisonment with a four-year stay of execution and a fine of ¥1 million.79

Information theft from an educational company

In July 2014, it was revealed that the customer information of an educational company (Benesse Corporation) had been stolen and sold to third parties by employees of an outsourcing contractor of the educational company. In September 2014, the Ministry of Economy, Trade and Industry promulgated an administrative guidance requesting that the educational company reform its security control measures and supervision of outsourcing contractors (in respect of violation of the duty regarding security control measures under Article 20 APPI. There was also found to be a violation of the duty regarding the supervision of an outsourcing contractor under Article 22 APPI). Benesse Corporation actually distributed a premium ticket (with a value of ¥500) to its customers to compensate for the damage incurred by the customers. Currently, however, a lawsuit is pending before the Supreme Court brought by a customer requesting damages of ¥100,000 (Osaka High Court dismissed the customer’s claim). On 29 October 2017, the Supreme Court sent the case back to Osaka High Court for further examination, holding that Osaka High Court erred in stating that any concern over the leak of personal information without any monetary damage is insufficient to establish any damage against the appellant (customer) under Article 709 of the Civil Code. At the time of writing, it is anticipated that Osaka High Court will hand

---

75 3-3-2 of the APPI Guidelines, p. 41.
77 Announcement No. 695 of 31 August 2004 by the MIC.
down a new decision clarifying the liability of businesses handling personal information for the leaking of customer’s personal information and a method of calculating the amount of damages arising from the information leak.

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

As stated in Section IV, it is generally considered that when an entity handling personal information in Japan obtains personal information from business operators outside Japan or assigns personal information to business operators outside Japan, the APPI is applicable to the entity handling personal information in Japan. The amended APPI requires that business operators obtain consent from the principal for international transfers of personal data. However, foreign business operators may circumvent this restriction by implementing proper and reasonable measures to protect personal information in accordance with the standards provided by the APPI.

IX CYBERSECURITY AND DATA BREACHES

i Cybersecurity

The amendments to the Criminal Code, effective since 14 July 2011, were enacted to prevent and prosecute cybercrimes. Since under the previous law it was difficult to prosecute a person who merely stored a computer virus in his or her computer for the purpose of providing or distributing it to the computers of others, a person who not only actively creates, provides or distributes a computer virus, but also who acquires or stores a computer virus for the purpose of providing or distributing it to the computers of others without justification, may not be held criminally liable under the amendments.

Following the 2011 amendments, three primary types of behaviours are considered as cybercrimes: the creation or provision of a computer virus; the release of a computer virus; and the acquisition or storage of a computer virus. The Act on the Prohibition of Unauthorised Computer Access (APUCA) was also amended on 31 March 2012 and took effect in May of that year. The APUCA identified additional criminal activities, such as the unlawful acquisition of a data subject’s user ID or password for the purpose of unauthorised computer access, and the provision of a data subject’s user ID or password to a third party without justification.

Following a 2004 review, the government has begun developing essential functions and frameworks aimed at addressing information security issues. For example, the National Information Security Centre was established on 25 April 2005, and the Information Security Policy Council was established under the aegis of an IT Strategic Headquarters (itself part of the Cabinet) on 30 May 2005.

80 Act No. 45 of 1907, Amendment: Act No. 74 of 2011.
82 Review of the Role and Functions of the Government in terms of Measures to Address Information Security Issues (IT Strategic Headquarters, 7 December 2004).
Finally, the Basic Act on Cybersecurity, which provides the fundamental framework of cybersecurity policy in Japan, was passed in 2014.84

**ii Data security breach**

There is no express provision in the APPI creating an obligation to notify data subjects or data authorities in the event of a data security breach. However, the APPI Guidelines stipulate that actions to be taken in response to data breach, etc. should be set out separately from the Guidelines. The PPC has set out desirable actions as follows:85

1. Internal report on the data breach, etc. and measures to prevent expansion of the damage;
2. Investigation into any cause of the data breach, etc.;
3. Confirmation of the scope of those affected by the data breach, etc.;
4. Consideration and implementation of preventive measures;
5. Notifications to any person (to whom the personal information belongs) affected by the data breach etc.;
6. Prompt public announcement of the facts of the data breach, etc. and preventive measures to be taken; and
7. Prompt notifications to the PPC about the facts of the data breach, etc. and preventive measures to be taken except for where the data breach, etc. has caused no actual, or only minor, harm (e.g., wrong transmissions of facsimiles or emails that do not include personal data other than names of senders and receivers).

In addition, the PPC has the authority to collect reports from, or advise, instruct or give orders to, the data controllers.86

An organisation that is involved in a data breach may, depending on the circumstances, be subject to the suspension, closure or cancellation of the whole or part of its business operations, an administrative fine, penalty or sanction, civil actions and class actions or a criminal prosecution.

**X OUTLOOK**

**i The future development of the amended APPI**

As stated in Section II, the amended APPI, which entered fully into force in May 2017, has drastically changed the legal framework for the protection of personal information in Japan. As of this writing, there have as yet been no leading cases or new matters to which the amended APPI applies and, led by the PPC, new practices based upon the new framework have just started. It is anticipated that the role of the PPC will be central to the new privacy policy in Japan and thus special attention should be paid to its activities for insight into the future development of the amended APPI.

---

84 Act No. 104 of 12 November 2014.
85 PPC Announcement No.1 of 2017.
86 Articles 40–42 APPI.
The judicial reaction to the leaking of personal information in Japan

As stated in Section VII, an important data breach case (Benesse Corporation) is currently pending before Osaka High Court and its decision (and its subsequent Supreme Court decision, if any) may articulate the scope of the obligations of business operators handling personal information and the calculation of damages arising from data breaches in Japan.
I OVERVIEW

The Personal Data Protection Act 2010 (PDPA), which came into force on 15 November 2013, sets out a comprehensive cross-sectoral framework for the protection of personal data in relation to commercial transactions.

The PDPA was seen as a key enabler to strengthen consumer confidence in electronic commerce and business transactions given the rising number of cases of credit card fraud, identity theft and selling of personal data without customer consent. Before the PDPA, data protection obligations were spread out among certain sectoral secrecy and confidentiality obligations, while personal information was primarily protected as confidential information through contractual obligations or civil actions for breach of confidence.

The PDPA imposes strict requirements on any person who collects or processes personal data (data users) and grants individual rights to ‘data subjects’. Enforced by the Commissioner of the Department of Personal Data Protection (the Commissioner), it is based on a set of data protection principles akin to that found in the Data Protection Directive 95/46/EC of the European Union (EU)\(^2\) and, for this reason, the PDPA is often described as European-style privacy law. An important limitation to the PDPA is that it does not apply to the federal and state governments.\(^3\)

The processing of information by a credit reporting agency is also exempted from the PDPA. In the past, credit reporting agencies did not fall under the purview of any regulatory authority in Malaysia, drawing heavy criticism for inaccurate credit information reporting. The Credit Reporting Agencies Act 2010, which came into force on 15 January 2014, now provides for the registration of persons carrying on credit reporting businesses under the regulatory oversight of the Registrar Office of Credit Reporting Agencies, a division under the Ministry of Finance, which is charged with developing a regulated and structured credit information sharing industry.

---

1 Shanthi Kandiah is a partner at SK Chambers. She was assisted in writing this chapter by Aida Harun and Carmen Koay, associates at SK Chambers.

2 The EU Data Protection Directive 95/46/EC has now been replaced with the EU General Data Protection Regulation, which came into force on 25 May 2018.

3 There is some ambiguity about which public entities fall within this definition. It does not appear that agencies and statutory bodies established under Acts of Parliament or state enactments to perform specific public functions, such as Bank Negara Malaysia (BNM), the Employees Provident Fund, the Securities Commission Malaysia and the Companies Commission of Malaysia, fall within the scope of this exemption.
i  **Cybersecurity**

The PDPA enumerates the security principle as one of its data protection principles. Under this principle, an organisation must ensure both technical and organisational security measures are well in place to safeguard the personally identifiable information that it processes. The ISO/IEC 27001 Information Security Management System (ISMS), an international standard, which deals with information technology systems risks such as hacker attacks, viruses, malware and data theft, is the leading standard for cyber risk management in Malaysia.

Sectoral regulators such as BNM and the Securities Commission Malaysia have also been actively tackling issues relating to cybersecurity in relation to their relevant sectors by issuing guidelines and setting standards for compliance (discussed in Section IX).

The intersection between privacy and cybersecurity also manifests in the extent of the tolerance for government surveillance activity: the PDPA does not constrain government access to personal data, as discussed in Section VI. The reasons given to justify broad government access and use include national security, law enforcement and the combating of terrorism.

II  **THE YEAR IN REVIEW**

The most significant development this year that has affected and will continue to affect the legal landscape in Malaysia is the installation of a new federal government following the outcome of the Malaysian general elections held on 9 May 2018. The new Minister of Communications and Multimedia (Mr Gobind Singh Deo) has signalled firm commitment to enforcement against data breaches, ordering follow-up action on cases of personal data breaches that had received significant media attention.

To date, the Commission’s enforcement actions tend towards enforcement of straightforward breaches. As at June 2018, there are now at least five enforcement cases that have resulted in conviction by the court and at least another eight cases that are expected to be tried in court. A majority of the convictions are for the offence of processing personal data breaches that had received significant media attention.

Several organisations in the following sectors have also received inspection visits from the Commissioner’s office: utility, insurance, healthcare, banking, education, direct selling, tourism and hospitality, real estate and services (retail and wholesale). Section 101 of the PDPA gives the Commissioner power to inspect the personal data systems in corporations with a view to making recommendations on compliance. The organisation is given limited notice of the pending visit. If an organisation fails to make the necessary improvements post-inspection, this could lead to criminal enforcement action under the PDPA. An inspection visit from the Commissioner’s staff will entail a detailed review of the following areas:

- personal data collection forms and privacy notice;
- internal standard operating procedures for personal data management within the organisation;
- person in charge of personal data management within the organisation and his or her awareness of the legal requirements; and

---

4 Section 16(4) of the PDPA.
Complaints remain the primary trigger for the investigation and enforcement activities of the Commissioner. As at June 2018, the Commissioner has received over 700 official complaints since the coming into force of the law. Unsurprisingly, a majority of complaints relate to processing of data in the electronic environment.\(^5\)

Cybersecurity issues have also received significant media attention as Malaysian companies were not spared in the global ransomware attacks, such as the WannaCry cyberattack in 2017. Currently, Malaysia does not have a specific law addressing cybersecurity-related offences. Enforcement agencies, such as the National Cybersecurity Agency (NCSA), have to rely on existing legislation, such as the Communications and Multimedia Act 1998 (CMA), the Defamation Act 1957 and the Sedition Act 1948, to combat cyberthreats.\(^6\)

### III REGULATORY FRAMEWORK

#### i Privacy and data protection legislation and standards

The PDPA is a comprehensive data protection legislation containing seven data protection principles, including the general principle establishing the legal requirements for processing personal data (e.g., with consent or in compliance with the legal requirements), notice (internal privacy notices for employees and external notices for consumers), choice, disclosure, data security, integrity and retention, and rights of access. Failure by an organisation to observe these principles is an offence.\(^7\) The Personal Data Protection Standards 2015, which came into force on 23 December 2015 (the Standards) are considered the ‘minimum’ standards to be observed by companies in their handling of personal data of customers and employees, and failure to implement them carries criminal sanctions.

The PDPA also sets up a co-regulatory model that emphasises the development of enforceable industrial codes of practice for personal data protection against the backdrop of the legal requirements of the government. Codes of Practice that have been approved and registered by the Commissioner include the Personal Data Protection Code of Practice for the Utilities Sector (Electricity),\(^8\) the Personal Data Protection Code of Practice for the Insurance/Takaful Industry\(^9\) and the Personal Data Protection Code of Practice for the Banking and Financial Sector.\(^10\) Additional codes of practice – one for the communications sector and one for legal practitioners – are also expected to be introduced sometime this year.

As the Codes set sector-specific prescriptions, it is likely that these will set the expected standards for the specific sector, over and above the Standards. Non-compliance with the codes will also carry penal consequences.\(^11\)

---

5 Meeting with officers of the Commissioner at the Personal Data Protection Department in Putrajaya on 9 July 2018.
6 See Section IX.i.
7 Section 5(2) of the PDPA.
8 With effect from 23 June 2016.
9 With effect from 23 December 2016.
10 With effect from 19 January 2017.
11 Section 29 of the PDPA.
**Personal data**

Three conditions must be fulfilled for any data to be considered as ‘personal data’ within the ambit of the PDPA.\(^{12}\)

First, the data must be in respect of commercial transactions. ‘Commercial transactions’ is defined under the PDPA as transactions of a commercial nature, whether contractual or not, and includes any matter relating to the supply or exchange of goods or services, agency, investments, financing, banking and insurance.\(^{13}\) There is some ambiguity as to whether an activity must have a profit motivation to be considered a commercial transaction.

Second, the information must be processed or recorded electronically or recorded as part of a filing system.

Third, the information must relate directly or indirectly to a data subject who is identifiable from the information or other information in the possession of the data user. A central issue for the application of the PDPA is the extent to which information can be linked to a particular person. If data elements used to identify the individual are removed, the remaining data becomes non-personal information, and the PDPA will not apply.\(^{14}\)

**Sensitive personal data**

Sensitive personal data is defined as any personal data consisting of information as to:

- the physical or mental health or condition of a data subject;
- his or her political opinions;
- his or her religious beliefs or other beliefs of a similar nature;
- the commission or alleged commission by him or her of any offence; or
- any other personal data as the minister responsible for personal data protection (currently the Minister of Communications and Multimedia) may determine.\(^ {15}\)

Sensitive personal data may only be processed with the explicit consent of the data subject and in the limited circumstances set out in the PDPA.\(^ {16}\)

**Application of the PDPA**

The PDPA applies to any person who processes or has control over the processing of any personal data in respect of commercial transactions.

‘Processing’ has been defined widely under the PDPA to cover activities that are normally carried out on personal data, including collecting, recording or storing personal data, or carrying out various operations such as organising, adapting, altering, retrieving, using, disclosing and disseminating the data. The prevailing view with respect to social media companies which have established a presence in Malaysia (for example through opening a branch office in Malaysia), is that they will be regarded as a data user and be subject to the PDPA for any data which they process in Malaysia (such as the personal data of their employees). Data processed wholly outside of Malaysia may not fall within the purview of the PDPA. In this connection, there appears to be some doubt about the application of

---

12 Section 2 of the PDPA.
13 Section 2 of the PDPA.
14 See also Section 45(1)(c) of the PDPA.
15 Section 2 of the PDPA.
16 Section 40(1) of the PDPA.
the PDPA to social media companies where it concerns data of users of social media if the interpretation taken is that this data is not being processed by the branch office in Malaysia or that no equipment in Malaysia is being used to process the data, except for the purpose of transit through Malaysia.17

A further point to note is that the PDPA only regulates personal data in the context of commercial transactions. As such, there is also some ambiguity as to whether a nominal user of social media (i.e., for recreational and social use) would enjoy the protection offered by the PDPA.

Most of the obligations under the PDPA apply to a ‘data user’ (i.e., ‘a person who either alone or jointly in common with other persons processes any personal data or has control over or authorises the processing of any personal data, but does not include a data processor’).

A ‘data processor’ who processes personal data solely on behalf of a data user is not bound directly by the provisions of the PDPA.

### ii General obligations for data users

#### Registration

The Personal Data Protection (Class of Data Users) Order 2013 lists 11 categories of data users who have to be registered with the Commissioner. The categories are:

- a banking and finance;
- b insurance;
- c telecommunications;
- d utilities;
- e healthcare;
- f hospitality and tourism;
- g education;
- h real estate and property development;
- i direct selling;
- j services (e.g., legal, accountancy, business consultancy, engineering, architecture, employment agencies, transportation); and
- k retail and wholesale.

The list of data users was expanded in 2016 to include two additional sectors: pawnbroking and money lending.18 Failure to register by these categories of data users is an offence.19

#### Purpose limitation

A data user may not process personal data unless it is for a lawful purpose directly related to the activity of the data user, the processing is necessary and directly related to the purpose, and the personal data are adequate and not excessive in relation to that purpose.

The data subject must also consent to the processing of the personal data unless the processing is necessary for specific exempted purposes.20

---

17 Section 2(2) of the PDPA
18 Personal Data Protection (Class of Data Users) (Amendment) Order 2016, which came into effect on 16 December 2016.
19 Section 16(4) of the PDPA.
20 Section 6(2) of the PDPA.
Consent
The PDPA does not define ‘consent’; nor does it prescribe any formalities in terms of the consent. However, the Personal Data Protection Regulations 2013 (the Regulations) provide that the data user must keep a record of consents from data subjects. The Regulations further provide that the Commissioner or an inspection officer may require production of the record of consents. It places the burden of proof for consent squarely on the data user.

Helpfully, the Personal Data Protection Code of Practice for the Utilities Sector (Electricity) provides examples of consent, whether express or implied, that must be recorded or maintained by the data user. These examples include:

a signatures, or a clickable box indicating consent;
b deemed consent;
c verbal consent; and
d consent by conduct or performance.

Consent is deemed given by way of conduct or performance if the data subject does not object to the processing; the data subject voluntarily discloses its personal data; or the data subject proceeds to use the services of the data user.

Verbal consent should be recorded digitally or via a written confirmation that consent was given.

Explicit consent
Regarding explicit consent, the Personal Data Protection Code of Practice for the Utilities Sector (Electricity) provides the following examples: where the data subject provides his or her identification card to be photocopied or scanned; where the data subject voluntarily provides the sensitive personal data; and verbal statements that have been recorded or maintained.

Notification
Data users are obliged to notify individuals of their purposes for the collection, use and disclosure of personal data on or before such collection, use or disclosure. For example, where a data user intends to use personal information collected for a different purpose, such as marketing communications, the data user must provide the affected individuals with the choice to disagree with the purpose before doing so.

Disclosure
Data users shall not disclose personal data for any purpose other than that for which the data was disclosed at the time of collection, or for a purpose directly related to it; or to any party other than a third party of the class notified by the data user without a data subject’s consent.21

Retention
Personal data should not be kept longer than necessary. Retention policies must take into account any relevant requirements imposed by applicable legislation. However, the Standards appear to impose organisational requirements that may be challenging for organisations to

---

21 If a data user is found guilty of disclosing personal data without the consent of the data subject, he or she may be liable to a 300,000-ringgit fine or two years’ imprisonment, or both.
comply with. Personal data collection forms are required to be destroyed within a period of 14 days, unless the forms can be said to have some ‘legal value’ in connection with the commercial transaction. It is unlikely that this time frame would be feasible for most organisations.

A record of destruction should be properly kept and be made available when requested by the Commissioner.

**Data subjects’ rights**

A data subject has various rights to his or her personal data kept by data users. These are:

- the right of access to personal data;  
- the right to correct personal data;  
- the right to withdraw consent;  
- the right to prevent processing likely to cause damage or distress;  
- the right to prevent processing for purposes of direct marketing.

**iii Technological innovation**

In general, the regulatory framework has not developed specific rules (outside the application of the seven principles in the PDPA) to deal with data privacy issues created by cookies, online tracking, cloud computing, the internet of things or big data.

Government efforts appear to be focused on positioning the country appropriately to benefit from these innovations. For example, the Ministry of Science, Technology and Innovation has unveiled the National Internet of Things Strategic Roadmap (the Roadmap). Under the Roadmap, a centralised regulatory and certification body will be established to address privacy, security, quality and standardisation concerns.

**iv Specific regulatory areas**

There are special confidentiality rules that apply to data in specific sectors, such as the banking and financial institutions sectors, the healthcare sector as well as the telecommunications and multimedia sectors. However, these rules do not comprehensively cover all aspects of data protection in the comprehensive manner addressed by the PDPA, which tracks the information life cycle from its collection and use through to its storage, destruction or disclosure.

**Minors**

The PDPA does not contain specific protection for minors (below the age of 18). Section 4 of the PDPA states that for minors, the guardian or person who has parental responsibility for the minor shall be entitled to give consent on behalf of the minor.

22 Section 30 of the PDPA.
23 Section 34 of the PDPA.
24 Section 38 of the PDPA.
25 Section 42 of the PDPA.
26 Section 43 of the PDPA.
Financial institutions
A banker’s duty of secrecy in Malaysia is statutory as is clearly provided under Section 133(1) of the Financial Services Act 2013 (FSA). The duty is not absolute. Section 153 of the FSA provides the legal basis for BNM to share a document or information on financial institutions with an overseas supervisory authority.

The Guidelines on Data Management and MIS Framework issued by BNM sets out high-level guiding principles on sound data management and MIS practices that should be followed by financial institutions. It is noteworthy that boards of directors and senior management are specifically entrusted with the duty to put in place a corporate culture that reinforces the importance of data integrity.

Healthcare
The Medical Act 1971 is silent on the duty of confidentiality. The Confidentiality Guidelines issued by the Malaysian Medical Council in October 2011 after the PDPA was enacted are the most comprehensive articulation of the confidentiality obligation of health professionals.

Multimedia and telecommunications
The General Consumer Code of Practice (GCC), developed by the Communications and Multimedia Consumer Forum of Malaysia, sets out a number of consumer protection principles, one of which is the protection of consumers’ personal information (quite similar in scope to the seven PDPA principles) for the telecommunications and multimedia sectors. The GCC binds all licensed service providers under the CMA and all non-licensed service providers who are members of the Consumer Forum.

Direct selling
The PDPA prescribes direct sellers as one of the 11 classes of data users that must register with the Personal Data Protection Department.

The PDPA also gives consumers the right to request in writing that the direct seller stop or not begin processing their personal data. Failure to cease using personal data for direct marketing purposes after a data subject has objected could make the offender liable for a fine of up to 200,000 ringgit, imprisonment for up to two years, or both.

IV INTERNATIONAL DATA TRANSFER AND DATA LOCALISATION
Section 129(1) of the PDPA states that a company may only transfer personal data out of Malaysia if the country is specified by the Minister of Communications and Multimedia Malaysia and this is then published in the Gazette. The Commissioner had issued a Public Consultation Paper entitled Personal Data Protection (Transfer of Personal Data To Places Outside Malaysia) Order 2017 (the Proposed Order 2017), which seeks feedback from the public on the Commissioner’s draft whitelist of countries to which the personal data

27 Schedule 11 of the FSA sets out a list of permitted disclosures.
28 See also Section 165 of the Islamic Financial Services Act 2013.
29 Management Information System.
30 The Malaysian Communications and Multimedia Content Code also sets out privacy related restrictions.
31 (PCP) No. 1/2017.
originating in Malaysia may be freely transferred without having to rely on exemptions provided by Section 129(3) of the PDPA. The places identified in the Proposed Order 2017 are as follows: European Economic Area member countries, the United Kingdom, the United States, Canada, Switzerland, New Zealand, Argentina, Uruguay, Andorra, the Faroe Islands, Guernsey, Israel, the Isle of Man, Jersey, Australia, Japan, Korea, China, Hong Kong, Taiwan, Singapore, the Philippines and Dubai International Financial Centre.

As at June 2018, the Proposed Order 2017 has yet to be gazetted. Until it comes into effect, to transfer data outside the country, organisations will have to rely on the exemptions set out in Section 129(3) PDPA, which include:

a where the data subject has consented to the transfer;
b where the transfer is necessary for the performance of a contract between the data subject and the data user;
c where the transfer is necessary to protect the vital interests of the data subject; and
d where the data user has ‘taken all reasonable precautions and exercised all due diligence’ to ensure that the personal data will not be processed in the recipient country in a way that would be a contravention of the PDPA.

Unlike EU law, Malaysian law does not require transfer contracts to be made for the benefit of third parties. Malaysia also has a doctrine of privity of contract that prevents enforcement of third-party benefits by data subjects.

V COMPANY POLICIES AND PRACTICES

Organisations are under the obligation to implement policies and enforce certain practices to ensure their compliance with the PDPA.

i Data protection officers

The requirements for a data protection officer are not mandated under the law. However, the Commissioner’s Proposal Paper (No. 2/2014), Guidelines on Compliance with Personal Data Protection 2010, makes a clear proposal for every organisation to establish responsibility for protection of personal data at the highest level and to designate an officer for this responsibility. The officer’s primary responsibility will be to ensure that all policies, procedures, systems and operations are aligned with the PDPA. There is, however, no requirement for a senior management position such as a chief privacy officer.

In addition, the proposed Guidelines appear to place the responsibility for protection of personal data at the highest level, which would appear to suggest that privacy should be a board level issue.

ii Online privacy policies

It is not uncommon for an organisation’s privacy policy to be used as a privacy notice. Privacy policies are sometimes used as a privacy notice in lieu of developing a separate document.

iii Internal privacy policies for employees’ rights and responsibilities

The notice and choice principle requires an employer to inform the employee of the nature of the information collected; whether the information will be shared with a third party; and that he or she has the right to access the information collected.
iv Requirement for data privacy due diligence and oversight over third parties
The Standards require data users, in discharging the security principle, to bind third parties contractually to ensure the safety of personal data from misuse, loss, modification, unauthorised access and disclosure. Some organisations do take the additional step of reserving audit rights over third parties processing personal data of their behalf, but this is not currently mandated.

v Written information security plan
The Regulations require that data users develop and implement a security policy for their companies. This security policy must comply with standards established by the Commissioner from time to time. Some of the more prescriptive standards for implementation are the standards stipulating that the transfer of personal data through removable media devices (e.g., USB thumb drives) and cloud computing services (e.g., Dropbox and Google Drive) is no longer permitted, unless authorised in writing by the ‘top management’ of the company.

Even when permitted, each transfer of personal data via such a removable media device must be recorded. Additionally, data users are required to record access to personal data, and to make the records available to the Commissioner upon request.

vi Incident response plan
Data breach management and incident response plans have not been mandated by the Commissioner.

VI DISCOVERY AND DISCLOSURE
The data protection provisions under the PDPA do not affect any rights and obligations under other laws. There is a clear exemption for disclosure of personal data for a purpose other than the purpose for which data was collected where the disclosure is necessary for the purpose of preventing or detecting a crime, or for the purpose of investigations.

In this regard, Malaysian legislation (including the PDPA) tends to provide authorities with extensive powers of search and seizure, including powers to search without a warrant. This power arises where the delay in obtaining a search warrant is reasonably likely to adversely affect investigation, or where evidence runs the risk of being tampered with, removed or destroyed.

Section 263(2) of the CMA is particularly noteworthy. Internet service providers as licensees under the CMA must comply with the Malaysian Communications and Multimedia Commission or any other authorities that make a written request for their assistance in preventing an offence or the attempt of any crime listed under Malaysian law.

Section 263(2) is broad enough to permit authorities to gain access to telecommunications information such as contact information and content of communications.

32 The Personal Data Protection Standards 2015.
VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

The Commissioner has been entrusted with certain powers under the PDPA to enforce the PDPA. It has conferred powers to carry out inspections and investigations on data users, whether or not these are initiated by any complaints received from the public. The powers of the Commissioner include:

- conducting inspections on data users’ personal data systems;
- publishing reports that set out any recommendations arising from the inspections; and
- serving enforcement notices on data users for a breach of any of the provisions of the PDPA, and directing data users to take (or refrain from taking) specified steps to ensure that they comply with the PDPA.

The Commissioner’s authorised public officers also have various powers of enforcement under the PDPA, including:

- conducting investigations on the commission of any offence under the PDPA;
- conducting searches and seizure of data users’ computerised data, documents, equipment, systems and properties, with or without a warrant;
- requiring the production of computers, books, accounts, computerised data or other documents kept by data users; and
- arresting without warrant any person who the authorised public officer reasonably believes has committed or is attempting to commit an offence under the PDPA.

It is worth highlighting a provision that is now commonplace in Malaysian legislation (including the PDPA) that provides that where an offence is committed by a body corporate, its director, chief executive officer, chief operating officer, manager, secretary or other similar officer, the entity or person may be deemed to have committed the offence unless it, he or she can establish that there was no knowledge of the contravention, and that it, he or she has exercised all reasonable precautions and due diligence to prevent the commission of the offence.33

ii Recent enforcement cases

In early 2018, an online employment agency was convicted and fined 10,000 ringgit for processing personal data without a certificate of registration. This is the second case involving an employment agency in the services sector that has led to a conviction.34

iii Private litigation

The PDPA does not provide for a statutory civil right of action for breach of any of the provisions of the PDPA. An aggrieved individual can nevertheless still pursue a civil action under common law or tort against a data user who has misused the individual’s personal data.

33 Section 133(1) of the PDPA.
VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

The PDPA applies to all activities relating to the collection, use and disclosure of personal data in Malaysia. As such, it will also apply to foreign entities processing such data in Malaysia regardless of whether they have an actual physical presence in Malaysia. The PDPA does not apply to personal data that is processed outside Malaysia, unless the data is intended to be further processed in Malaysia.

IX CYBERSECURITY AND DATA BREACHES

Statistics from Cybersecurity Malaysia for 2018 – MyCERT Incident Statistics – indicate that from January to May 2018 alone there have been over 2,713 reports on cyber-related incidents. This figure does not include those cases that go unreported almost daily, as there is no requirement to report breaches to the authorities or to customers.

The National Cybersecurity Policy is Malaysia’s integrated cybersecurity implementation strategy to ensure the critical national information infrastructure (CNII) is protected to a level that is commensurate with the risks faced. Cutting across government machineries, the implementation has drawn in various ministries and agencies to work together to create a CNII that is secure, resilient and self-reliant. Implementation of this scheme has involved certification of CNIIIs by Cybersecurity Malaysia to be ISMS-compliant. Other initiatives include Cyber999 Help Centre, which is a service operated by the Malaysian Computer Emergency Response Team (MyCERT) for internet users to report or escalate computer security incidents.

BNM has also issued a circular on ‘Managing Cybersecurity Risks’, under which financial institutions are required to adhere to the ‘Minimum Measures To Mitigate Cyberthreats’. Measures include measures to:

- assess the implementation of multi-layered security architecture;
- ensure security controls for server-to-server external network connections;
- ensure the effectiveness of the monitoring undertaken by Security Operation Centre to view security events, including incidents of all security devices and critical servers on a 24/7 basis; and
- subscribe to reputable threat intelligence services to identify emerging cyberthreats, uncover new cyberattack techniques and provide counter measures.

The Securities Commission Malaysia has also issued its Guidelines on Management of Cyber Risk, which sets out a framework to address cybersecurity resilience for capital market participants’ management of cybersecurity risks.

i Cyberlaws

In contrast to the comprehensive approach of the PDPA, Malaysia’s cyberlaws are scattered across various pieces of legislation. Presently, the key provisions of Malaysia’s cyberlaws are as follows.

---

36 With effect from 31 October 2016.
CMA

Offences under the CMA include:

a the offence of the use of network facilities or network services by a person to transmit any communication that is deemed to be offensive and that could cause annoyance to another person;\(^{37}\)

b the offence of using an apparatus or device without authority;\(^{38}\)

c the offence of improper use of network facilities or network services – such as annoying, abusive, threatening, harassing or obscene communications – emails (spamming), SMS or MMS website content publishing;\(^{39}\)

d the offence of interception and disclosure of communications;\(^ {40}\) and

e the offence of damage to network facilities.\(^ {41}\)

Other cyberoffences include:

a cyberpornography and exploitation of children;\(^ {42}\)

b online sedition and internet defamation;\(^ {43}\)

c misuse of computers;\(^ {44}\)

d prostitution and other illegal cybersexual activities; and

e cyberterrorism.\(^ {45}\)

ii Laws to facilitate prosecutions of internet-based offences

A noteworthy development in Malaysian law was the introduction of Section 114A into the Evidence Act 1950, which came into force on 31 July 2012. Under the new Section 114, a person is deemed to be a publisher of a content if it originates from his or her website, registered networks or data-processing device of an internet user unless he or she proves the contrary.

iii Laws to promote tracking transactions conducted on the internet

Examples of laws that provide for tracking and recording transactions conducted on the internet include the Cyber Centre and Cyber Cafe (Federal Territory of Kuala Lumpur) Rules 2012 and the Consumer Protection (Electronic Trade Transactions) Regulations 2012. The former requires any person operating a cybercafé and cybercentre to maintain a customer

---

37 Section 233(1)(a) of the CMA.
38 Section 231 of the CMA.
39 Section 233 of the CMA.
40 Section 234 of the CMA.
41 Section 235 of the CMA.
42 Sections 292, 293 and 294 of the Penal Code, Section 5 of the Film Censorship Act 2002 and Section 31 of the Child Act 2001.
43 Sections 3 and 4 of the Sedition Act 1948, Section 211 (prohibition on provision of offensive content) and Section 233 (improper use of network facilities or network service) of the CMA.
44 Section 3 (unauthorised access to computer materials), Section 4 (unauthorised access with intent to commit or facilitate commission of further offence), Section 5 (unauthorised modification of contents of any computer) and Section 6 (wrongful communications) of the Computer Crimes Act 1997.
45 The Penal Code contains provisions that deal with terrorism that may apply to cyberterrorism, such as Chapter VIA Sections 130B–130T (incorporated into the Penal Code on 6 March 2007).
entry record and a record of computer usage for each computer, whereas the latter require online business owners and operators to provide their full details and terms of conditions of sale, to rectify errors and maintain records.

**X OUTLOOK**

We expect to see more enforcement actions by the Commissioner in the coming year, particularly given the focus of the new Minister on enforcement of data breaches. Having said that, we expect to see the Commission continue to pursue its ‘audit’ type regulation (as opposed to prosecution) via inspection visits and enforcement notices as a means of instilling awareness amongst data users on their data protection obligations.

The Cambridge Analytica scandal in April 2018 received wide media coverage in Malaysia and is likely to have led to elevated awareness and concern among data subjects in Malaysia on their privacy rights, including the extent of use of their personal data by social media companies. This is said to be reflected through the high number of complaints from the public received by the office of the Commissioner this year. In light of this, it is possible that we will see more legal developments to regulate the internet and social media. Any ambiguity about the application of the PDPA to social media companies should be resolved as this is likely to be a recurring theme for user distress over data protection in the near future.

Compliance with the General Data Protection Regulation (GDPR), which came into force on 25 May 2018, is a topic we expect to see proactively addressed by Malaysian corporations that collect and process data of EU residents (such as customers, permanent residents, visitors and expatriates) given its extraterritorial reach and the potentially hefty fines that can be imposed due to breach. The GDPR’s prescriptions on organisational and technical measures to protect personal data are likely to influence Malaysian standard setting as well. For example, the office of the Commissioner has indicated that following the GDPR’s lead, data breach notification is likely to be made compulsory in Malaysia. A blanket requirement to report every breach could be excessively onerous. A threshold such as ‘a real risk of serious harm’ should accompany such a requirement (which would most certainly cover identity theft). In these cases, the breach notification should be made to the consumer. Alternatively, and instead of a mandatory requirement, Parliament may wish to consider explicitly recognising breach notification as a mitigation point in enforcement proceedings. This would not just address considerations on fairness to the consumer, but provide organisations with the incentive to advise consumers of breaches, as well as the flexibility to evaluate their position.

---

46 Maximum fine that can be imposed under the GDPR is 4 per cent of worldwide total annual turnover, or €20 million, whichever is higher.

47 Meeting with officers of the Commissioner at the Personal Data Protection Department in Putrajaya on 9 July 2018.
Chapter 18

MEXICO

César G Cruz-Ayala and Diego Acosta-Chin

I OVERVIEW

The right to privacy or intimacy is contemplated in Paragraphs 1 and 12 of Article 16 of the Mexican Constitution, which prohibits anyone from intruding onto an individual's person, family, domicile, documents or belongings (including any wiretapping of communication devices), except when ordered by a competent authority supported by the applicable law.

The right to data protection is stipulated in Paragraph 2 of Article 16 of the Constitution, which seeks to set a standard for all collecting, using, storing, divulging or transferring (collectively processing) of personal data (as defined below) to secure the right to privacy and self-determination. The right to privacy and data protection are closely related fundamental rights that, along with other fundamental rights, seek to protect individuals' ability to guard a portion of their lives from the intrusion of third parties. Notwithstanding this, while a breach of privacy usually results in a breach of the right to protection of personal data, a data protection breach does not always result in a breach of privacy.

The first formal effort to address personal data protection was introduced in 2002 when the Mexican Congress approved the Federal Law for Transparency and Access to Public Governmental Information (the Former Transparency Law). Although the Former Transparency Law was mainly aimed at securing access to any public information in the possession of the branches of government and any other federal governmental body, it also incorporated certain principles and standards for the protection of personal data being handled by those government agencies. This effort was followed by similar legislation at the state level.

After several attempts to address data protection rights more decisively, in 2009 Congress finally approved a crucial amendment to the Constitution that recognised the protection of personal data as a fundamental right. Consequently, Congress enacted the Federal Law for the Protection of Personal Data in Possession of Private Parties (the Private Data Protection Law), which became effective on 6 July 2010 and was followed by the Regulations of the Private Data Protection Law on 22 December 2011.

Additionally, in January 2014 Congress approved an amendment to the Constitution to create an autonomous entity to be in charge of enforcing the Private Data Protection Law and to take on the duties of the former Federal Institute for Access to Information and Protection of Data (the former IFAI), which was originally created as a semi-autonomous agency separate from the federal public administration. However, in a rather controversial move, the former IFAI amended its internal regulations so that it could assume the necessary

1 César G Cruz-Ayala is a partner and Diego Acosta-Chin is an associate at Santamarina y Steta, SC.
characteristics, and role, of the proposed autonomous entity. Consequently – and as a result of the new General Law for Transparency and Access to Public Governmental Information, which annulled the effect of the former Transparency Law – all matters previously dealt with by the former IFAI are now being handled by the ‘new IFAI’ as an autonomous entity; and it has adopted the title National Institute of Transparency, Access to Information and Protection of Personal Data (INAI).

The Private Data Protection Law is an omnibus data protection law that sets the principles and minimum standards that shall be followed by all private parties when processing any personal data. However, the Private Data Protection Law also recognises that standards for implementing data protection may vary depending on the industry or sector; accordingly, the Private Data Protection Law can certainly be complemented by sectorial laws and self-imposed regulatory schemes, which would focus on particular industry standards and requirements, to the extent that those standards and requirements comply with the data protection principles in the Private Data Protection Law. There have been efforts to promote such sector-specific rules among those processing any personal data within the same industry.

Finally, on 13 December 2016 the Mexican Congress approved the General Law for the Protection of Personal Data in Possession of Governmental Entities (the Governmental Data Protection Law, and collectively with the Private Data Protection Law, the Data Protection Laws), which was enacted on 27 January 2017, to establish a legal framework for the protection of personal data by any authority, entity or organ of the executive, legislative and judicial branches, political parties, and trust and public funds operating at federal, state and municipal level. On the understanding that this particular publication is intended to address issues arising from data protection in the private sector, we will not address in detail the governmental Data Protection Law, unless it is necessary to add context.

The INAI is in charge of promoting the rights to protection of personal data, and enforcing and supervising compliance with the Data Protection Laws and those secondary provisions deriving from those Laws. To this end, with respect to the private sector, the INAI has been authorised to supervise and verify compliance with the Private Data Protection Law; interpret administrative aspects of the Data Protection Laws; and resolve claims and, inter alia, impose fines and penalties. The INAI has been actively working through media campaigns to raise awareness among corporations and individuals of the relevance of adequate protection of personal data. Although the INAI has the authority to initiate enforcement activities, most fines and penalties imposed have resulted from claims filed by data subjects. We are aware that companies that have been fined by the INAI for breaching the Private Data Protection Law have challenged the decisions by means of nullity claims and amparo lawsuits; however, the relevant files are not publicly available.

II THE YEAR IN REVIEW

During 2018, the INAI continued to enforce the Private Data Protection Law at a slower pace but at the same time issued more guidelines intended to protect personal data when using technological means.

On 23 April 2018 INAI, published in the Federal Official Gazette an agreement that modifies the electronic system to file DPPs (as defined below) and complaints for the protection of rights. As a result of such amendment, this system allows: (1) private entities to review resolutions imposing sanctions; (2) submittal of any documents associated with a proceeding; and (3) private entities to access information about the status of a proceeding.
On 28 May 2018, the INAI issued a non-binding guideline to assist data controllers in the processing of biometric data in compliance with the Private Data Protection Law. Such guideline reaffirms the criteria about what data is deemed as ‘personal data’ or ‘sensitive personal data’ by explaining that biometric data would be considered as personal data when it directly identifies a person or allows the identification of a person, and as sensitive personal data when (1) such refers to the most intimate sphere of a data subject; (2) undue use can lead to discrimination; and (3) illegitimate use results in material risk to the data subject.

On May 2018 several banks in Mexico suffered a major cyberattack on their Interbank Electronic Payments System (SPEI), and approximately 400 million Mexican pesos were stolen. From the information publicly available, it appears that money was stolen from accounts owned by the banks and not by accountholders. The Attorney General Office (PGR) is still conducting an investigation on such cyberattack. INAI is also investigating if such attack constitutes a data breach.

It was published on 12 June 2018 in the Federal Official Gazette the approval of the Mexican Senate to adhere to the Convention for Protection of Individuals with regard to Automatic Processing of Personal Data dated 28 January 1981 (Convention 108) and its additional Protocol dated 8 November 2001 (ETS 181), which will enter into force on 1 October 2018. The Mexican government is now committed through Convention 108 and ETS 181 to take necessary measures to give effect to the provisions of said Convention, and, therefore, it is foreseeable that a bill may be submitted in the near future to amend the Data Protection Laws. As of the time of writing, Mexico has not yet adhered to the Additional Protocol of Convention 108 that was approved by the Committee of Ministers of the Council of Europe on 18 May 2018 (ETS 223) since such is still open for signing until 10 October 2018.

On 15 July 2018 INAI published a bulleted informing that it would initiate a proceeding to impose penalties against the data controller operating in Mexico the application ‘Pig.gi’. Although there is limited public information, we understand that the investigation against said company was initiated ex officio by INAI, considering that (1) the respective privacy notice does not include all of the elements described in the Private Data Protection Law; (2) the data controller processed users’ personal data for purposes that are not described in their privacy notice; and (3) failed to implement those means necessary to comply with data protection principles, such as responsibility and legality.

On 16 July 2018, INAI published certain recommendations to assist data controllers in preventing theft of personal data while using public Wi-Fi networks to reduce risks associated with undue processing of personal data.

On July 2018, INAI published a certain non-binding guideline to protect personal data while using social media applications. Among other matters, such guideline provides instructions and recommendations about access control and consent for applications, webpages, and games, as well as suggestions to protect personal data when interacting in any social media.

Although the General Data Protection Regulations (GDPR) applicable in the European Union (EU) are not enforceable per se in Mexico, some provisions of GDPR are intended to address processing beyond the borders of the EU, to the extent such processing is with respect to personal data of EU citizens or residents or EU Member States. As a result of the above, it is foreseeable that (1) those entities that intend to carry on any business operation in the EU (even through remote means), shall meet with these new standards imposed by the GDPR;
and (2) those Mexican companies whose parent company is headquartered in the EU, or process personal data on behalf of those EU companies or subsidiaries, may be asked to meet with these new standards imposed by the GDPR.

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

The most relevant pieces of legislation addressing personal data protection in Mexico are the following:

a. the Constitution;
b. the Private Data Protection Law;
c. the Governmental Data Protection Law;
d. the Regulations of the Private Data Protection Law;
e. the Guidelines for Privacy Notices; and
f. the Self-Regulation Parameters on Data Protection, which are applicable to the private sector.

The Private Data Protection Law identifies those data protection principles governing all processing of personal data, as well as the obligations imposed on any private person, whether an individual or entity, that has control over the processing of personal data (a data controller), data processors (as defined below), third parties and any others engaged in the processing of personal data. As demanded by the Private Data Protection Law, the Mexican executive branch issued the Regulations of the Private Data Protection Law with the intention of clarifying the scope of those principles and obligations provided by the Private Data Protection Law. The Regulations also set out the rules applicable to the exercise by data subjects of their rights in relation to data controllers and those proceedings arising from claims before the INAI filed by data subjects in the event of a breach of the Private Data Protection Law by a data controller. Finally, the Guidelines for Privacy Notices (the Guidelines), issued by the Secretariat of the Economy, set the standard of detail that should be met by data controllers when drafting their own privacy notices and the scope of the language in privacy notices, and the Self-Regulation Parameters on Data Protection establish the rules, criteria and procedures for the development and implementation of self-regulatory schemes on data protection, and were also issued by the Secretariat of the Economy.

Both the Federal Consumer Protection Law and Federal Consumer Protection Law for the Users of Financial Services also contain stipulations protecting consumers, whether individuals or entities, from any processing of their information for marketing purposes. Corporations or financial entities that wish to market products must first review the list of consumers who do not wish to receive marketing information and recorded in the Public Registry of Consumers held by the Federal Consumers Attorney's Office (Profeco), or the Public Registry of Individual Users, which is managed by the National Commission for the Protection of Financial Services Users (Condusef). Any marketing activity with any consumers enrolled in the registries may result in fines by Profeco or Condusef, as applicable.

Key definitions

In addition to any other terms defined herein, the following terms in particular should be taken into consideration for a better understanding of Mexican law on the subject:
a data processor: any natural person or entity that individually or jointly with others carries out the processing of personal data on behalf of the data controller;
b data subject: the natural person whom the personal data concerns;
c personal data: any information related to an identified or identifiable individual. The following information would not be subject to the Private Data Protection Law:
• information collected and stored for personal use and not intended for divulgence or commercialisation;
• information collected by credit bureaux;
• information about entities;
• information about any individual when acting as a merchant or professional practitioner; and
• information about any individual when rendering services to a legal entity or to a merchant or professional practitioner, provided that information is limited to the subject’s name, duties or position, business address, business email, business telephone and business facsimile, and the information is processed when representing the merchant or professional practitioner;
d public access source: a database that may be accessed by anyone without complying with any requirement, except for the payment of a fee;
e sensitive personal data: personal data affecting the most intimate sphere of the data subject, or of which the misuse may be a cause for discrimination or great risk for the data subject, such as information regarding racial or ethnic origins, political opinions, religious beliefs, trade union membership, physical or mental health, and sex life;
f transfer: any kind of communication of personal data made to a person other than the controller, data processor or data subject; and
g remittance: any kind of communication of personal data between the data controller and the data processor, within or outside Mexican territory.

**Data protection principles**

In consideration of the fact that the Private Data Protection Law is inspired by the European model provided in 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 free movement of such data, the backbone of the Private Data Protection Law lies in the principles by which each data controller must abide to protect the personal data being processed by the same. These principles are summarised as follows.
a Legality: all personal data shall be lawfully collected and processed, and its collection shall not be made through fraudulent or deceitful means.
b Consent: all processing of personal data shall be subject to the consent (whether express or implied) of the data subject, with certain exemptions set out in the Private Data Protection Law. If it is not exempted, when a data controller is processing any sensitive personal data, the data controller must obtain the express consent of the data subject to process this data, which must be evidenced in writing or through an electronic signature or any other authentication mechanism developed for that purpose. Exemptions to the requirement to obtain consent exist when:
• processing is permitted by law;
• the personal data are publicly available;
• processing prevents association between the personal data and the data subject or his or her identification because of the structure, content or grade of disaggregation of the personal data;
• processing is intended to comply with obligations resulting from a legal relationship between the data controller and the data subject;
• there is an emergency situation that may injure an individual or damage his or her assets;
• processing is essential for the purposes of rendering healthcare services or assistance, the application of preventive medicine, determination of medical diagnosis or the management of healthcare services, as long as the data subject is unable, in the terms provided by the General Health Law, to grant his or her consent for the applicable procedure; and
• a competent authority orders the processing.

c Quality: the data controller shall cause personal data in a database to be relevant, accurate and up to date for the purpose for which it is meant to be used, and shall only retain personal data for as long as is necessary to fulfil the specified purpose or purposes.

d Purpose: processing of personal data shall be limited to the purpose or purposes specified in the privacy notice. No database containing sensitive personal data shall be created without justifying that the purpose for its collection is legitimate, concrete and in compliance with those activities or explicit purposes sought by the data controller. Any processing of personal data for a purpose that is not compatible or analogous to what is set forth in the privacy notice shall require a new consent from the data subject.

e Proportionality: processing of personal data must be necessary, adequate and relevant for the purpose or purposes set forth in the privacy notice. With respect to sensitive personal data, reasonable efforts shall be made to keep the period of processing to a minimum.

f Loyalty: processing of personal data shall favour the interests of the data subject and a reasonable expectation of privacy, which shall be understood as the level of confidence that any person deposits in another that the personal data exchange between them shall be processed as agreed between them in compliance with the Private Data Protection Law.

g Transparency: data controllers shall inform data subjects, by means of a privacy notice, about the personal data that will be subject to processing, and the purpose or purposes for the processing. With respect to sensitive personal data, the privacy notice shall expressly state that the information is of a sensitive nature.

h Responsibility: data controllers shall adopt the necessary measures to comply with all data protection principles during the processing of personal data, even if the processing is carried out by data processors or third parties. Therefore, a data controller shall ensure full compliance with the privacy notice delivered to the data subject by that data controller or by third parties with whom it has a legal relationship.

In addition to the aforementioned principles, all data controllers shall comply with the duties of security and confidence, which are also applicable to data processors and third parties receiving any personal data from a data controller, in which case the latter must verify that these duties are observed by the third parties concerned.
Data controllers shall implement appropriate organisational, technical and physical security measures to protect personal data against unauthorised damage, loss, modification, destruction, access or processing. These measures shall be at least equivalent to those implemented for their own confidential information.

Further, all personal data shall be kept confidential, even upon the termination of any relationship with the data subject.

Compliance

INAI has *ex officio* authority to supervise compliance with the Private Data Protection Law, to date, many proceedings to verify compliance have resulted from claims filed by data subjects, however, INAI determined to initiate *ex officio* proceedings when deemed appropriate.

ii General obligations for data handlers

Although a data controller must comply with each and all of the principles described above (see Section III.i), the most basic obligations imposed on data controllers are mainly the drafting of privacy notices and making these available to data subjects, as well as gathering consent with the processing of personal data, unless exempted under the Private Data Protection Law.

The drafting and delivery of the privacy notice to a data subject constitutes a key factor in complying with the principle of transparency described above and, therefore, there are no exemptions to the same. As a result of the above, the privacy notice must be drafted complying with strict standards and requirements stipulated in the Private Data Protection Law, its Regulations and, particularly, the Guidelines. There are three types of privacy notices whose general characteristics, terms and conditions are as follows:

- **full**: a full privacy notice must be used when the personal data is personally collected from a data subject, and must contain all elements contained in the corresponding provisions of the Private Data Protection Law, the Regulations and the Guidelines;
- **simplified**: a simplified privacy notice may be used when the personal data are collected directly but using remote means from the data subject and must contain all elements contained in the corresponding provisions of the Private Data Protection Law, the Regulations and the Guidelines; and
- **abbreviated**: an abbreviated privacy notice may be used when personal data is directly obtained from a data subject by printed means and when the personal data collected is minimal. It must be drafted in accordance with Article 28 of the Regulations and Guideline 38 of the Guidelines.

When drafting the privacy notice, data controllers must identify the different uses intended for the personal data, and also distinguish those uses required for the legal relationship between the data controller and data subject (necessary purposes) from those that are not (secondary purposes). This requirement is important considering that a data subject may choose to reject (or in the future withdraw consent for) processing for those secondary purposes without affecting his or her relationship with the data controller.

When required, consent for processing any personal data must be obtained upon the collection of the personal data if the collection is made personally or directly from the data subject, or before any processing if personal data was not collected by the data controller directly from the data subject.
Data subjects also have the following rights, which are meant to secure protection of personal data (the ARCO rights):

- **a** access: a data subject is entitled to access his or her personal data held by a data controller, as well as to know the privacy notice to which processing is subject;

- **b** rectification: a data subject is entitled to rectify his or her personal data when it is inaccurate or incomplete;

- **c** cancellation: a data subject shall always be entitled to cancel his or her personal data. The cancellation of personal data implies that the information shall be kept by the data controller as long as required under the applicable legal relationship or once that time has elapsed, the data controller shall delete the corresponding personal data, unless otherwise requires by an applicable statute; and

- **d** opposition: a data subject shall always be entitled, with legal cause, to oppose the processing of his or her data. If a data subject does so, the data controller shall not be entitled to process the data concerning that data subject.

Notwithstanding the above, and in addition to the ARCO rights, the data subject shall also be entitled to withdraw consent (withdrawal), either in whole or in part, with respect to the processing of personal data, and may limit the use or divulgement of personal data (data limitation), and, collectively with the ARCO rights and the right of withdrawal (data claims), by opting out mechanisms or enrolling in lists kept by the data controller, or of Profeco or Condusef, of those data subjects unwilling to receive marketing communications. The data controller shall describe the means available to the data subject to exercise any of the data claims. Data claims shall be exercised free of charge, unless the data subject exercises the same claim to access personal data within a period of 12 months, in which case the data controller may charge a fee that shall not exceed three times the unit for measure and update (UMA) in force. Unfortunately, the creation of awareness in Mexico regarding the protecting of personal data is still a major challenge, considering that the lack of knowledge (and, in some cases, interest) together with the degree of specialisation of this matter may be delaying proper compliance with the Private Data Protection Law. Many data controllers are still gaining interest and experience in these matters, which has caused inadequate implementation of privacy notices, since this requires adequately mapping all data being processed to assess all implications. It is still common to see data controllers drafting their privacy notices without considering whether they are in fact processing any personal data, and to what extent.

### iii Specific regulatory areas

Notwithstanding the fact that the Private Data Protection Law is applicable to all private parties processing personal data, with certain exceptions, and that the Governmental Data Protection Law is enforceable in respect of any processing carried out by public agencies, Mexican Official Standard NOM-004-SSA3-2012 regarding medical records is currently the only extant industry- or sector-specific legal framework – despite the idea fostered by the Private Data Protection Law that laws or regulations applicable to specific sectors or industries should be enacted. Among other relevant provision made by this standard, it defines the concept of ‘clinical records’ and imposes obligations of confidentiality in respect of these records; health providers and establishments that gather, manage and store clinical records are required to implement all measures necessary to maintain this confidentiality (e.g., password-protected firewalls).
iii Technological innovation and privacy law

Technological innovations pose a challenge under the Private Data Protection Law, as this area is broadly and scarcely regulated, with no specific rules applicable to processing affected by such developments. Concepts such as ‘big-data analytics’ and the ‘internet of things’ have not yet been defined under the Private Data Protection Law or other applicable data protection legislation. However, processing of personal data using any technological innovation (including the use of remote or local communications media or any other technology) is governed by the Private Data Protection Law, therefore the challenge lies in determining the degree of applicability of that Law, given that the data subject must be informed of the processing. When using remote or local communications media or any other technology, notification must be given to the data subject through a visible communication or warning about the use of those technologies to process his or her personal data, and about the manner in which the technological mechanism may be disabled (unless its use is fundamental for technical reasons). This information must be also included in the full privacy notice, clearly identifying the personal data being collected by that means, as well as the purpose of the collection. In addition, notwithstanding that the concept of biometric data is not defined under the Private Data Protection Law or other applicable data protection legislation, the non-binding guideline issued by INAI defines biometric data and reaffirms that biometric data is deemed ‘personal data’ or ‘sensitive personal data’.

IV INTERNATIONAL DATA TRANSFER AND DATA LOCALISATION

Mexico is party to several international organisations (such as APEC – the Asia-Pacific Economic Cooperation – and the Organization of American States) that aim to protect personal data being transferred within their respective regions, whether domestically or internationally. Convention 108 and ETS 181 establishes that the parties shall adopt provisions and restrictions for the transfer of personal data between the parties subject to such convention and non-party countries.

Under the Private Data Protection Law, an international communication of personal data originating from a data controller subject to the Private Data Protection Law may be deemed either a ‘transfer’ or a ‘remittance’, depending on the purpose for communicating the data and the recipient of the same. Each of these communications must meet specific requirements, which are described below.

i Transfer of personal data

A transfer is any communication of personal data by a data controller to any private or public entity different from the data subject or the data processor. In this regard, any transfer of personal data must be consented to by the data subject concerned, except where exempted pursuant to Article 37 of the Private Data Protection Law; the transfer must be notified to the data subject by means of a privacy notice and limited to those purposes justifying the transfer.

A data controller would be able to transfer personal data without the consent of a data subject if the transfer is:

a stipulated by a law or treaty to which Mexico is party;
b needed for prevention of illness or medical diagnosis, healthcare assistance, medical treatment or management of health services;
c made to holding companies, subsidiaries or affiliates under common control of the data controller who operate under the same processes and internal policies;
required by an agreement entered into or to be entered into between the data controller and a third party in the interest of the data subject;

necessary or legally required to protect the public interest or the prosecution or enforcement of justice;

required for the acknowledgment, exercise or defence of a right in a judicial proceeding;
or

necessary for the preservation of, or compliance with, a legal relationship between the data controller and the data subject.

Any international data transfer shall be evidenced by an agreement or any other document whereby the third party assumes the same data protection obligations undertaken by the data controller and the conditions for processing as consented to by the data subject as detailed in the corresponding privacy notice. International data transfers do not need the approval of the INAI or any other Mexican regulatory agency to be completed and there is no need to submit standard contractual clauses or comparable instruments to any of them; however, a data controller may seek, at its sole discretion, the opinion of the INAI on whether an international transfer complies with these applicable requirements before completing such transfer.

ii Remittance of personal data

A remittance is any communication of personal data made by a data controller to an individual or legal entity that is unrelated to the data controller with the purpose of conducting any processing on behalf of the data controller.

A remittance does not need to be notified to a data subject by means of a privacy notice, nor does it require the consent of the data subject. However, to carry out the remittance, a data controller and data processor shall enter into a certain agreement with the purpose of evidencing the existence, scope and content of the relationship, which should be consistent with the privacy notice delivered by the data controller to the relevant data subject.

Under the GDPR, certain restrictions or requirements may have to be fulfilled prior to completion of an international transfer of personal data to data controllers or data processors located in Mexico. Notwithstanding the approval of the Convention 108 and ETS 181, as of the date of our review, Mexico has not been recognised by the European Commission as a third country providing adequate data protection to facilitate personal data transfers to countries within the EU.

V COMPANY POLICIES AND PRACTICES

The following are among the security measures data controllers must implement:

a carry out data mapping to identify the personal data that are subject to processing and the procedures involving in the processing;

b establish the posts and roles of those officers involved in the processing of the personal data;

c identify risk and carry out a risk assessment when processing personal data;

d implement security measures;

e carry out a gap analysis to verify those security measures for which implementation is still pending;

f develop a plan to implement those security measures that are still pending;
g implement audits;

h conduct training for those officers involved in the processing;

i have a record of the means used to store personal data; and

j put in place a procedure to anticipate and mitigate any risks arising from the implementation of new products, services, technologies and business plans when processing personal data.

VI DISCOVERY AND DISCLOSURE

Data controllers are obliged to disclose personal data in the event that there is a binding and non-appealable resolution from a competent Mexican authority. A data subject’s consent for the processing of personal data shall not be required to the extent that the processing is meant to comply with a resolution from a competent Mexican authority. The Constitution grants all individuals the fundamental right to protect their personal data, as well as the right to access, rectify, cancel and oppose any processing of the same. It should be noted that the Constitution recognises that this right is not without limit; therefore, those principles protecting personal data are subject to certain exceptions for national security, public policy, public security and health, or to protect third-party rights.

Transfers of personal data for legal proceedings or investigations in other countries shall always be carried out in compliance with the Private Data Protection Law and through a letter rogatory following the adequate diplomatic or judicial channels. Data controllers should always analyse whether the privacy notice was disclosed to the data subject, whether the consent is required or exempted and was properly granted, and whether the transfer is limited to those purposes used to justify it. Additionally, the data controller and the relevant authority should enter into an agreement or any other document, as described in Section IV.

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

Initiation of proceedings

The INAI takes charge of data protection proceedings (DPPs) and of compliance-verification proceedings (VPs).

DPPs are intended to resolve claims filed by a data subject or his or her legal representative alleging that a data controller has failed to attend to a claim exercising the data subject’s ARCO rights or when the resolution of the data controller does not satisfy the data subject.

VPs may be commenced ex officio by the INAI or at the request of a party. An ex officio VP will take place following a breach of a resolution issued in connection with a DPP, or if a breach of the Private Data Protection Law is presumed to be founded and substantiated by the INAI. During a VP, the INAI shall have access to the information and documentation deemed necessary, in accordance with the resolution originating the verification.

Penalties

In the event that the INAI becomes aware during a DPP or VP of a presumed breach of the Private Data Protection Law, a proceeding to impose penalties will commence assessing the infringement. The available penalties include the following:
Mexico

A warning issued by the INAI urging a data controller to comply with the data subject’s demands. Note that this course of action is limited to certain types of infringement; fines representing an amount of between 100 and 320,000 times the UMA, which is published by the National Institute of Statistics and Geography, which will be determined based on the nature of the infringement; and imprisonment for up to three years in certain cases, such as when someone authorised to process any personal data causes a security breach in relation to the data under his or her control with the purpose of obtaining a gain; or imprisonment for up to five years when someone processes personal data with the intention of obtaining a gain by deceiving, or taking advantage of the error of, a data subject or the person authorised to transfer any personal data.

The penalties set out in (b) and (c) above may be doubled if the infringement involves sensitive personal data. Although the Private Data Protection Law does not entitle a data subject to receive any indemnification in light of damage suffered because of a data controller’s breach, it does acknowledge that any of the fines or penalties indicated above would be imposed against a data controller without prejudice to any liability that the data controller may have in civil and criminal law.

When assessing the fine or penalty to be imposed, the INAI would consider:

- the nature of the personal data;
- the inappropriateness of the failure to comply with the claim of the data subject;
- whether the action or omission was deliberate;
- the economic capacity of the data controller; and
- any reoccurrence of the breach.

Data controllers may challenge these sanctions or fines by means of a nullity claim before the Federal Court of Tax and Administrative Justice.

In addition, Profeco and Condusef are entitled to verify the adequate use of consumer information. If either of them finds that a corporation is engaging in unsolicited marketing to a customer enrolled in the Public Registry of Consumers or the Public Registry of Individual Users, or that it has used consumers’ data for a purpose other than marketing, the following shall apply: as of 2017, Profeco may impose fines of up to 1.56 million Mexican pesos; or Condusef may impose fines of up to 2,000 times the UMA in force.

In recent years, the INAI has fined, inter alia, financial institutions, telecom companies and healthcare providers. The most significant fines imposed by the INAI so far are discussed below. However, most of these fines have been challenged by the data controllers concerned and the proceedings are pending resolution.

**Tarjetas Banamex**

A fine of 9.8 million Mexican pesos was imposed on Tarjetas Banamex, SA de CV SOFOM, ER (Tarjetas Banamex) on the grounds that Tarjetas Banamex personnel made telephone calls to collect an unpaid balance but to a telephone number belonging to a data subject that was different from the cardholder in question, and failed to allow the data subject to rectify

---

2 Between 8,060 and 25,792,000 Mexican pesos in 2018.
3 161,200 Mexican pesos in 2018.

© 2018 Law Business Research Ltd
and cancel his personal data stored with Tarjetas Banamex. This resolution has been removed from INAI’s webpage, as a result of a preventive measure issued by the Federal Fiscal and Administrative Court.

**Hospital**
A fine of 4.6 million Mexican pesos was imposed to Operadora de Hospitales Ángeles, SA de CV (the hospital) on the grounds that the hospital was negligent when processing and answering a claim filed by a data subject to request access to her clinical file. Given that the clinical file contained sensitive personal data of the data subject, the fine was doubled.

**Telcel**
A fine of 10.2 million Mexican pesos was imposed on Radiomóvil Dipsa, SA de CV (Telcel). Telcel personnel had made calls to collect unpaid balances from individuals who were on a frequently dialled-number list of persons owing money to Telcel, and divulged to them the amount owed without the express consent of the data subject.

**Banorte**
A fine of 32 million Mexican pesos was imposed on Banco Mercantil del Norte, SA, Institución de Banca Múltiple, Grupo Financiero Banorte (Banorte). Banorte collected sensitive personal data without the consent of the data subject and stored the data without a legal justification in breach of the principles of information, proportionality and legality, as it failed to deliver a privacy notice to the claimant and processed personal data of the husband of the claimant that was not necessary, adequate or relevant for the purpose of the data collection.

**Recent enforcement cases**
A fine of 1.402 million Mexican pesos was imposed to a travel agency. The INAI’s decision to fine the travel agency was based on the following arguments:

a. the travel agency obstructed INAI’s verification proceeding, by failing to answer the official requirements for information;

b. the travel agency privacy notice did not comply with the Private Data Protection Law;

c. the travel agency processed personal data, including financial information of the data subject, without the express consent of the data subject; and

d. the travel agency processed personal data from the data subject in breach of the principles of information, responsibility and legality, since it failed to deliver its privacy notice to the data subject and processed personal data in contravention of the Private Data Protection Law.

A fine of 35,050 Mexican pesos was imposed on a fitness club. The INAI’s decision to fine the fitness club was based on the following arguments:

a. fingerprints are biometric data and constitute sensitive personal data, therefore the fitness club collected the data without the written consent of the data subject;

b. the fitness club privacy notice did not comply with the Private Data Protection Law; and
the fitness club processed personal data from the claimant in breach of the principles of information, responsibility and legality, since the fitness club failed to deliver its privacy notice to the claimant, did not adopt adequate security measures and processed personal data in contravention of the Private Data Protection Law.

iii Private litigation
The Private Data Protection Law makes no provision regarding remedies or financial recovery for the data subject as a result of a breach of data protection rights; however, data subjects are entitled to file a claim before the civil courts to seek indemnification resulting from moral damage. We are not aware of any claims of this nature. The first chamber of the Mexican Supreme Court has issued certain ground breaking, non-binding court precedents resolving that, when awarding damages, courts and judges shall considering aggravating factors, such as the degree of responsibility, to determine a fair indemnification, thereby openly recognising concepts such as 'punitive damages', which were not developed in court precedents.

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS
The Private Data Protection Law is applicable to:

a data processors not located in Mexico, but that process personal data on behalf of data controllers located in Mexico;

b data controllers that are not located in Mexico, but that are subject to Mexican laws as a result of an agreement or in terms of international laws; or

c data controllers using means located in Mexico (even if they are not established in Mexico), except if those means are merely for transit purposes, without involving the processing of personal data.

As a result of the above, foreign companies must always analyse whether their activities, or the activities of their affiliates, would result in the application of the Private Data Protection Law.

Foreign companies have also faced certain challenges considering that, under the premise that privacy notices should be simple and easy to understand, the INAI has been reluctant to accept privacy notices issued by multiple data controllers, even if they are part of the same corporate group.

IX CYBERSECURITY AND DATA BREACHES
Cybersecurity is broadly addressed within the Private Data Protection Law and its Regulations, by establishing that all private entities processing personal data, and data controllers in particular, shall have adequate physical, technical and organisational measures to prevent any personal data breach. It should be noted that the Private Data Protection Law and its Regulations do not attempt to impose a catalogue of security measures to be adopted by those bound by them, but rather outlines general principles applicable to security measures that shall be implemented by those processing personal data. In that spirit, the INAI has issued certain documents in an attempt to simplify the implementation of security measures, such as:

a the Recommendations on Personal Data Security outlining the minimum actions needed to securely process personal data;

b the Methodology for Analysing Risk to assess the risks when processing personal data;
The Guide to Implementing a Personal Data Security Management System to establish security measures based on the cyclic model of ‘planning, doing, checking and acting’; and

the Guide on Personal Data Security for Micro, Small and Medium-Sized Businesses, which guides such companies in compliance with the Private Data Protection Law and its Regulations with respect to security measures and the implementation of a personal data security management system.

A data controller must notify each data subject upon confirmation that a data breach has occurred, once it has taken any actions intended to assess the magnitude of the breach. The notice shall contain at least the nature of the incident, the personal data affected, advice on the actions that may be adopted by the data subject to protect his or her interests, the remedial actions that were immediately carried out and the means through which the data subject may obtain further information. In addition, the data controller would have to take corrective and preventive actions and improve its security measures to avoid the reoccurrence of the same breach.

The Private Data Protection Law and its Regulations do not oblige a data controller to notify the INAI upon the occurrence of a breach or of the measures taken by the data controller. However, failing to comply with any of the obligations mentioned above may constitute an infraction under the Private Data Protection Law that may result in the imposition of sanctions by the INAI.

### OUTLOOK

We are not aware of any intended amendments to the Private Data Protection Law since the previous edition of this publication; however, we anticipate that a bill will be submitted in order to harmonise the Data Protection Laws with the Convention 108 and ETS 181.
I OVERVIEW

When it comes to protection of privacy and personal data, Poland has followed the EU standards and laws for many years and, in addition to the entry into force of the Polish Act on Personal Data Protection (the Act) on 10 May 2018, the country prepared its legal framework for the introduction of the General Data Protection Regulation (GDPR). There is still some room for improvement (e.g., how fast data privacy matters are dealt with by the data protection authority), but it seems that this is not a Poland-specific issue. Further legislative works are, however, needed, for example, in banking and insurance law.

Data protection officers and experts are in high demand in both the public and private sectors. Several higher-education bodies offer postgraduate studies focused on privacy and there are GDPR events on a daily basis. The awareness in society regarding privacy is high and probably increasing, owing to the fact that the GDPR is directly applicable. The e-Privacy regulation is also likely to increase this demand.

New legislation, not necessarily connected to the GDPR, was enacted in the previous year or will be enacted soon, including a law on counterrorism and preventing hate speech on the internet. From many perspectives, and for different reasons, privacy is a topical issue and although there are still aspects that are expected to be regulated in the near future, there are some who say it is already an overregulated area.

II THE YEAR IN REVIEW

Between the end of 2017 and the first half of 2018 we have seen a strong focus on preparing the Polish legal framework for the implementation of the GDPR. The Ministry of Digital Affairs, which is responsible for the introduction of the GDPR into Polish law, published several drafts of the amended Act in February and March 2018. The draft Act was eventually put forward for consideration by the Polish parliament on 5 April 2018 and was adopted on 10 May 2018 and is now fully binding. In parallel to the adoption of the Act, the draft on the amendment of certain acts in connection with ensuring compliance with the GDPR has not yet been adopted into the Polish legal framework. It is still being worked on by the Council of Ministers. We point out that some of those sectoral provisions were incorporated

1 Anna Kobylańska and Marcin Lewoszewski are partners, and Maja Karczewska and Aneta Miśkowiec are associates at Kobylańska & Lewoszewski Kancelaria Prawna Sp J.

and adopted in the Act, such as labour law, local government and banking law provisions. The basic and most needed provisions have been adopted and implemented in compliance with the GDPR.

Entities responsible for the implementation of the GDPR in Poland as well as private entities, such as lawyers, businesses and entrepreneurs, conducted trainings, lectures and events in order to familiarise themselves with the GDPR and its practical implementation.

In connection with the necessity to implement the NIS Directive, work on the draft law on the national cybersecurity system began on 8 January 2018 and was redirected to the Polish parliament on 30 April 2018. The last step taken towards the adoption of the above-mentioned was taken on 5 July 2018, which was the third and last reading at a Polish legislative proceeding. The Act on the National Cybersecurity System was signed by the President of Poland on 1 September 2018 and is now binding.

III REGULATORY FRAMEWORK

Privacy and data protection legislation and standards

Privacy law has its roots in the Constitution of the Republic of Poland of 2 April 1997, and in particular in Article 47, which guarantees the right of every citizen to a private life. This constitutional principle was further specified in Articles 23 and 24 of the Act of 13 April 1964 of the Civil Code, which protect the personal interests of natural persons.

Poland implemented EU Directive 95/46/EC by enacting the Act of 29 August 1997 on the Protection of Personal Data (the Act on the Protection of Personal Data). The Act on the Protection of Personal Data followed the EU Directive and was in compliance with EU law. It was of a general nature and regulated the whole spectrum of processing of personal data by the entities to which the Act on the Protection of Personal Data applied (including public bodies, associations, individual entrepreneurs and legal entities conducting businesses). The Act on Protection of Personal Data (from 1997) as from 25 May 2018 is not binding.

As of now, Poland is directly subject to provisions of the GDPR. However, it was necessary to adjust the national data protection provisions to new regulations and obligations resulting from the GDPR. Therefore, the Act, fully compliant with the GDPR, was adopted on 10 May 2018.

Data protection is also guaranteed by many sector-specific regulations. There are key legal acts covering data protection in the areas of banking law, insurance law, telecommunications, e-commerce, pharmaceuticals and health law, and other areas where sector-specific provisions

---

regulating how data should be processed are present. As was stated before, sectoral regulations will be amended to bring them into line with the GDPR. Nevertheless, the legislative procedure has not yet been completed.

Notwithstanding this regulatory spread, it seems that the President of the Office of Personal Data Protection (PUODO (the name of the supervisory authority was changed by the Act; the previous name was the General Inspector of Personal Data Protection)) has been less active when it comes to enforcement actions and inspections. According to publicly available statistics, in the first half of 2018 (so before the entry into force of the GDPR), PUODO conducted 21 inspections (compared with 212 in 2017). There is no information on the number of received complaints in 2018. In comparison, in 2017 there were 2,950 submitted complaints.

ii General obligations for data handlers

A controller, when processing personal data, has to ensure:

a. legal grounds for personal data processing;
b. limitation of purposes for which personal data are processed;
c. time limitation of personal data storage;
d. relevancy, accuracy and adequacy of the personal data processed by the controller;
e. enforcement of data subjects’ rights; and
f. security of the personal data.

Legal grounds for personal data processing include, among others, consent of a data subject, necessity to exercise a contract with the data subject, necessity of exercising rights or duties arising from law, and legitimate interests. The controllers often ask data subjects to grant their consent but, in fact, all other legal grounds should also be taken into account. Consent of a data subject may be easily withdrawn (at any time after its granting), so it is always worth considering other legal grounds for personal data processing.

The controller is obliged to fulfil an information obligation to inform data subjects about their rights. This information is provided at the first moment the data is gathered by the controller. The information should include: identity and contact details of the controller or data protection officer, the purpose and legal basis of the data collection, data recipients or categories of data recipient, possible transfer of personal data, storage period, whether the provision of personal data is a statutory or contractual requirement, the existence of rights to request from the controller as well as the right to lodge a complaint and information on the existence of automated decision-making, including profiling. Even more categories of information have to be provided in a situation where the personal data are not collected directly from the data subject.

If the controller outsources areas of its business, including personal data processing, it is obliged to ensure the outsourced third party (called a processor) takes proper care of the data. For this reason, the controller is obliged to enter into a data-processing agreement with the processor. The data processing agreement should include a provision obliging the processor to process the data solely within the scope of, and for the purpose determined in, the contract as well as imposing an obligation on the processor to sufficiently guarantee implementation of appropriate technical and organisational measures.

---

In case of an obligation to designate a data protection officer the controller notifies PUODO of data protection officers’ designation providing contact details. The Act specifies that a person previously functioning as an information security administrator (under the Act on Personal Data Protection this was a similar position to a data protection officer) the date of application of the GDPR becomes by law the data protection officer. As a rule, the notification needs to be fulfilled within 14 days from date of designation. Notwithstanding, in a big simplification, transitional provisions of the Act indicate that if an information security administrator was not designated prior to application of the GDPR and the controller is obligated to designate a data protection officer, the notification needs to be fulfilled until 31 July 2018. However, if an information security administrator was designated and the same person will function as data protection officer or a different person will be designated as a data protection officer the notification needs to be fulfilled until 1 September 2018.

The controller is obliged to secure the personal data against loss or unauthorised access. For this reason, the controller has to apply organisational and technical means appropriate for the type of risk. Controllers are obliged to specify what technical and organisational measures are appropriate for their organisation as neither GDPR legislation nor the Act defines step by step what safeguards to implement.

### iii Technological innovation and privacy law

**Cookies**

Polish law on the use of cookies has been introduced as an implementation of EU directives. Storing information on a user’s computer, including the use of cookies, is allowed under the following conditions:9

- the user should be informed of the purpose of storing and using the information, and about the possibility of configuring the browser or service settings to set rules regarding the use of the information about the user;
- the user, after receiving this information, consents to this use of his or her data; and
- the information stored on the user’s computer does not cause a change in the settings of the user’s computer device or software.

Under Polish law, the consent of the user should not be implied. With respect to the consent for the use of information included in cookies, however, the law allows consent to be granted indirectly (by making a choice in a browser’s settings). In practice, website users get initial information on the use of cookies each time they open a new website (via a pop-up banner). It is possible to use a website without accepting the cookie policy; however, website owners often require users to click the ‘I understand’ button before enabling full use of the website.

Non-compliance with the cookie law may result in a financial penalty of up to 3 per cent of the infringer’s revenue from the previous year.10

---

Location tracking

In July 2017, GIODO (now PUODO) published a broad analysis of the impact of location tracking on privacy.\footnote{11} The analysis covers both the Act on the Protection of Personal Data and the GDPR.

According to the authority’s stated view, data collected with reference to location tracking should be considered personal data. Therefore, the general rules for processing such data should be applied. The key principles applying to location tracking are the principles of legality,\footnote{12} expediency,\footnote{13} adequacy,\footnote{14} substantive correctness,\footnote{15} timeliness,\footnote{16} and integrity and confidentiality.\footnote{17} PUODO considers consent of the individual concerned to be the key legal basis for such processing.

As stated within the analysis, just as telecoms operators process a particular device’s location using base stations, database owners with mapped Wi-Fi access points process personal data when calculating the location of a particular smart mobile device. By specifying both objectives and the means of such processing, these entities become controllers within the meaning of Article 4(7) of the GDPR.\footnote{18}

Electronic marketing

In terms of the Polish law regarding unsolicited commercial information, the rules of using electronic devices for marketing purposes became unclear. It is forbidden to send commercial information by means of electronic communication (including emails, text messages and internet communicators) without the user’s consent.\footnote{19} This prohibition is broadly interpreted: even a company logo or a marketing slogan used in an electronic signature may be treated as commercial information. Moreover, this prohibition relates not only to sending emails to private persons, but also to individuals who represent companies. There is also one more prohibition on the use of telecommunication devices or automated calling systems for direct marketing.\footnote{20} Under this law, companies cannot make phone calls or send emails or text messages with their offers without users’ prior consent. As a result of these two types of prohibition, companies started asking users to grant consent to these two types of action, causing annoyance and lack of understanding on the part of the users.

Spamming may be punished under five different acts of Polish law (the Act on Provision of Services by Electronic Means, the Act on Combating Unfair Competition, the Act on Combating Unfair Market Practices, the Act on Competition and Consumer Protection and the Telecommunications Law) with a maximum financial penalty of up to 10 per cent of the previous year’s turnover. In practice, spammers and cold callers are rarely punished for their actions.

\footnote{12} Article 23, Section 1(1) of the Act on the Protection of Personal Data.
\footnote{13} Article 23, Section 1(2) of the Act on the Protection of Personal Data.
\footnote{14} Article 26, Section 1(3) of the Act on the Protection of Personal Data.
\footnote{15} Article 26, Section 1(3) of the Act on the Protection of Personal Data.
\footnote{16} Article 23, Section 1(4) of the Act on the Protection of Personal Data.
\footnote{17} Article 36 of the Act on the Protection of Personal Data.
\footnote{19} Article 10 Section 1 of the Act of 18 July 2002 on Provision of Services by Electronic Means.
\footnote{20} Article 172 Section 1 of the Act of 16 July 2004 – Telecommunications Law.
The new rules on the use of electronic devices for marketing purposes are expected with the adoption of the EU ePrivacy Regulation.\textsuperscript{21}

\textbf{iv Specific regulatory areas}

One of the most difficult aspects of processing personal data under Polish law relates to the employer–employee relationship. It is common practice for employers to process as much data as possible about employees and candidate employees. However, Polish employment law limits the scope of data that can be processed in such cases. Article 22(1) of the Act of 26 June 1974 on the Labour Code\textsuperscript{22} – changed by the Act – provides a list of the data that an employer can request from an employee or candidate employee, including date of birth, education and employment records. Courts have confirmed that employers are not allowed to process data other than those specified in the Labour Code, even with the employee’s consent, because of possible resulting imbalances between the employer and the employee.

The other interesting aspect regarding the processing of candidate employees’ and employees’ concerns background checks. In practice, the verification of candidates’ past history is limited to the documents they present to the employer and to checking the references supplied (subject to certain conditions). In most parts of the private sector, it would be non-compliant to verify candidates’ criminal records, with an exception for cases such as the employment of bodyguards.

\textbf{IV INTERNATIONAL DATA TRANSFER AND DATA LOCALISATION}

As to the international data transfer, these issues are now regulated by the GDPR provisions. For now there are no specific laws regulating this matter in Poland, however, it should be noted that the legislative works undertaken owing to the GDPR’s entry into force are still not finished. Therefore, it cannot be excluded that such regulations will be introduced in Poland in the near future.

\textbf{V COMPANY POLICIES AND PRACTICES}

Under the Act, there are no requirements obliging the companies to adopt company policies in the meaning of specific documentation relating to personal data protection.

However, as to the company practices, the Act introduces a complex regulation of the matter of video surveillance in the workplace. It has to be highlighted that this issue had not been explicitly regulated in Polish law before and therefore it had been causing considerable uncertainty among Polish employers.

Pursuant to the relevant provisions of the Act, the employer is allowed to install video surveillance in case it is necessary to (1) ensure the safety of the employees; (2) protect property; (3) control the process of production; (4) protect the trade secrets, which disclosure might cause damage to the employer. However, in line with the purpose and storage limitation principles expressed in the GDPR, the employer is required to ensure that the registered image recordings shall be processed by the employer only for the purposes for which they


\textsuperscript{22} Journal of Laws 2014, Item 1502.
were collected, for a period not exceeding three months, in case the video recording is not evidence in legal proceedings or the employer has not been informed that it may be evidence in such proceedings. The employer is limited also as to the location of the video surveillance, owing to the provision of the Act that states that to lawfully install the video surveillance in sanitary rooms, cloakrooms, canteens, smoking rooms or premises made available to trade union organisations, the employer shall ensure that such monitoring is necessary for the allowed purposes and that it does not violate either the dignity and other personal rights of the employee or the principles of freedom and independence of the trade unions.

The Act places strong emphasis on the information obligation in the context of video surveillance in the workplace, imposing on the employer an obligation to regulate the purposes, scope and the way of use of the surveillance in collective agreements with trade unions or in the internal workplace policies. If there is no collective agreement or the employer is not obliged to set workplace regulations, this information shall be included in a notice given to the employees. In each case every employee shall be provided in writing with the aforementioned information before he or she starts to carry out the work duties, and if the employee is already carrying out work duties – at least two weeks before the launch of the video surveillance. The employer is also obliged to indicate the monitored rooms and areas in a clear and visible manner, through the use of appropriate signs or acoustic signals, no later than one day before the launch of the video surveillance. The Act explicitly states that the aforementioned obligations are without prejudice to the information obligation deriving from the GDPR provisions.

The Polish legislator decided to regulate also the issue of email correspondence surveillance conducted by the employers, which – unlike video monitoring – is allowed to be undertaken for the purpose of exercising control over the working time and the potential off-duty activities of the employees, as the relevant provision states that it may be introduced when it is necessary ‘to ensure the workflow enables full use of the working hours and proper use of work tools handed to the employee’. However, this kind of workplace surveillance is also facing some limits, as its conduct cannot infringe the privacy of correspondence and the personal rights of the employees. It should be noted, though, that the information obligations in case of email surveillance correspond to the obligations imposed on the employer in case of video surveillance.

It has to be noted that the sector-specific acts on data protection, whose aim is to adjust the regulations regarding different sectors of Polish economy to the GDPR requirements, are still being processed. Therefore, more specific regulations on company policies and practices are expected to be adopted in Poland in the near future.

VI DISCOVERY AND DISCLOSURE

As a general rule, for the purposes of criminal proceedings, courts and prosecutors may demand any information and documents that may be needed for proceedings, including documents that contain personal data. There are specific provisions of law that relate to revealing personal data for the purposes of criminal proceedings held by authorities from EU countries.23 Disclosing personal data to such authorities by Polish institution requires their initial verification as to accuracy and completeness. A disclosing institution may impose

---

23 Act of 16 September 2011 on Exchanging Information with Investigation Institutions from EU Countries.
certain requirements on data receivers, such as removing or anonymising personal data after a certain time, limiting the scope of personal data processed or refraining from informing data subjects about their personal data processing.

Apart from courts and prosecutors, there are numerous other authorities and institutions that may request a disclosure of information, such as the Polish Police Force, the Internal Security Agency, the Polish Foreign Intelligence Agency, the Polish Border Guard, the Military Intelligence and Military Counter-Intelligence Services, the Central Anti-Corruption Bureau and the Polish Military Police.

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

The Act indicates explicitly that the PUODO is the body responsible in Poland for data protection issues and that it is the Polish supervisory authority in the meaning of the GDPR.

The Act defines the scope of competence of PUODO, which involves among others (1) conducting proceedings on infringements of data protection laws and imposing administrative fines according to the relevant GDPR provisions, and (2) monitoring of compliance with the data protection laws. These tasks, consistent with the GDPR provisions, are thoroughly described in the Act, with relevant references to Polish applicable laws.

As to the proceedings on infringements of data protection laws, the Act indicates the manner, in which the Polish general administrative procedure shall be applied, taking into account the specificity of the data protection cases. The Act establishes also the procedure applicable to the monitoring of compliance conducted by PUODO, which may be conducted in particular in the form of inspection. An inspection can be performed only under numerous restrictions, which were imposed by the Polish legislator in order to assure the participation of the controlled entity or person and the transparency of the activities undertaken during a inspection. The scope of control is also limited as to its timeframe, locations subject to control and types of evidence that may be considered during a control.

It has to be highlighted that pursuant to the Act, unlawful or unauthorised processing of personal data constitutes a criminal offence, which may be prosecuted by the prosecutor and is punishable by a fine, restriction of liberty or imprisonment of up to two years. However, in case the personal data involved belongs to the special categories of data as understood in the Article 9 of the GDPR, the possible restriction of liberty or imprisonment sanction is increased to a maximum of three years. The Act establishes also criminal responsibility for frustrating or impeding an inspection regarding the compliance with data protection laws, and therefore such actions are penalised with a fine, restriction of liberty or imprisonment for up to two years.

ii Recent enforcement cases

As to the enforcement cases issued in 2018, there was an interesting case, in which the then Polish supervisory authority, GIODO, was considering the scope of the obligation to delete personal data from backups. Finally, it determined that erasure of data requires also erasure of all backups. However, it was noted that as backups are useful only provided their integrity is maintained, in practice difficulties may arise when a backup contains data that is supposed to be deleted, as well as some other data, that is being lawfully processed. In such case, the need to consider the interests of an individual whose data shall be deleted and of other persons who shall be granted access to their data is uppermost. It should be noted that this issue is
now explicitly regulated in the GDPR as to the processing activities conducted by a processor, which is required to delete all existing copies after the end of the provision of services relating to processing.

Another case concerned a company that sent notifications to their customers titled ‘Important information regarding actualisation of your personal data’, a few months before the GDPR started to be directly applicable. The notifications attracted the attention of the Polish supervisory authority, as the customers where requested not only to give their consent to processing of their data, but also to give their consent to online marketing and telemarketing, as well as to agree to make their personal data available for marketing purposes to the company’s business partners. What was crucial in the case was the fact that the notification included a request to tick all six checkboxes and provide the company with the actual contact data, as they stated that the company ‘is obliged to update them due to the new regulations’. A decision has not been issued in this case yet, however, in the light of the GDPR provisions, according to opinions expressed by the experts, it is probable that such consent to processing should not be perceived as freely given.

iii Private litigation

Private litigation in relation to privacy and personal data does not have much of a profile in Poland and case law is scarce in this field. Last year saw very limited proceedings related to infringement of privacy based on civil law and the right to dignity. One of the courts ordered, for example, that installing a CCTV camera in front of a private apartment does not infringe a neighbour’s right to privacy. As stated by the judge deciding the matter: ‘The applicable legal system also grants everyone the personal right to live in their apartment (home), free from disturbances and unrest, and the right to protect their property. These goods are subject to the same protection as the right to privacy.’

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

It has to be noted that owing to the GDPR being directly applicable, foreign organisations do not have to be too concerned with complying with Polish regulations, since data protection law has been unified in the majority of aspects.

However, the provisions of the recently adopted Act have to be taken into account, especially with regard to above-mentioned video surveillance in the workplace. There are also some other regulations that shall be considered, for example, the Polish Labour Code, which explicitly indicates the scope of data that may be requested by an employer in relation to the employment, as well as the scope of data that may be requested in the recruitment process. Therefore, all data processed in relation to the employment and recruitment processes that exceed the aforesaid remits shall be processed on the basis of the data subject’s consent. It has to be highlighted also that according to the applicable laws, all data protection documentation must be kept in Polish.

IX  CYBERSECURITY AND DATA BREACHES

i  Cybersecurity

On 5 July 2018, the Act on the National Cybersecurity System implementing the NIS Directive into the Polish legal framework was voted on by the legislative bodies and on 1 September 2018 it was signed by the President of Poland and is now binding.

The purpose of the Act is in particular to organise the national cybersecurity system and to indicate tasks and duties of the entities included in this cybersecurity system. The system imposes different obligations on the entities providing essential services, digital services providers, public entities as well as CSIRT MON, CSIRT NASK and CSIRT GOV. However, not all business entities are subject to the new law. Essential services operators are entities based in Poland, to whom the decision was issued recognising them as an essential service operator and those which belong to the sector and subsector indicated in Appendix 1 of the Act on the National Cybersecurity System. Appendix 1 indicates, among others, entities from the energy sector, transport providers, entities providing banking services or healthcare services. The operators’ task is to recognise, secure and remedy incidents that could carry risk. For the purpose of prevention, the operator collects all possible information about cybersecurity threats and in consequence applies preventive measures limiting incidents on cybersecurity.

The operator is obliged to appoint an appropriate contact person for communication with entities of the national cybersecurity system. It is necessary for essential services operators to conduct an audit of the security of the IT systems used to provide the services – at least once every two years.

The digital service provider is a legal person or an organisational unit without legal personality, having its registered office or management on the territory of Poland or a representative with an organisational unit in Poland that provides digital services. Exceptions to the above are microentrepreneurs and small entrepreneurs. Digital services – in accordance with Appendix 2 of the Act on the National Cybersecurity System – are online trading platforms, cloud-based service providers and internet search engines. The obligations of digital service providers are narrower than the obligations of key service operators.

In the scope of cybersecurity services, the Act indicates the possibility to outsource services based on a contract.

ii  Data breaches

The GDPR imposes a general obligation on the controllers regarding notifying data breaches to the relevant supervisory authorities. It also defines the elements that each notification has to include.

According to the Act, the PUODO may keep an IT system, by which the controllers shall be able to notify data breaches. The wording of the aforesaid provision suggests that keeping such system is optional and a controller is allowed to notify the supervisory authority also by traditional means. This conclusion was confirmed by a supervisory authority’s officer, who nevertheless made it clear that notifying data breaches by electronic means is highly recommended.

Therefore, on the PUODO’s website there is already an electronic form available, which is intended to be used while notifying a data breach, along with instructions for the controllers. It has to be stressed out that the scope of information required in the form is much broader than the scope of information determined in the GDPR.
For instance, regarding the nature of breach, the controller is required to provide information whether the breach is a data confidentiality breach, a data integrity breach, or a data accessibility breach, which the form briefly explains. The controller is obliged also to indicate what did the breach consist in, however, the form provides for some suggestions presented in a form of checkboxes. The form requires the controller to indicate whether the breach was caused by intentional or unintentional, internal or external action; as well as to provide additional description of the cause. The scope of information is broadened also in case of categories of data (owing to the requirement to classify them as e.g., ‘identification data’, ‘economic data’, ‘official documents’, etc). The form requires also from the controller providing detailed information as to the measures taken or proposed to address the data breach; in particular regarding the carried out or planned communication with data subjects, including the indication of the date and the means of the communication, number of data subjects, as well as providing the supervisory authority with the exact wording of the communication. The controller is also required to inform whether the breach has already been notified to foreign supervisory authorities and – if applicable – to indicate what kind of legal obligations were met by such notification.

As to the manner of notifying the data breach to the supervisory authority, it has to be mentioned that to settle official matters by electronic means in Poland, owning a trusted profile is necessary. A trusted profile is a free-of-charge method of confirming identity in electronic contacts with Polish administration. However, owing to the fact that obtaining a trusted profile requires going through a registration process, not all entrepreneurs use it. Nevertheless, owing to the approach adopted by PUODO, it can be assumed that the electronic procedure of notifying data breaches will enjoy wide popularity among the Polish entrepreneurs.

**X OUTLOOK**

Businesses operating in Poland look forward to sector-specific acts implementing amendments of certain sector provisions regarding data protection to ensure compliance of the national legal framework with the GDPR, which, alongside the latter, will constitute the final and complex version of the package of legal acts implementing the GDPR. This covers key business sectors, such as banking, insurance, telecommunications and e-commerce. The GDPR is also a game-changer for the regulator itself, as it will face new, sometimes complicated, procedures. We can expect to see some uncertainty in the area of privacy law in the coming years, and from many perspectives.

At the same time, we are still awaiting general regulation of cybersecurity and implementation of the NIS Directive. Data breaches are also becoming more and more difficult to prevent, and the state and businesses should have proper tools to defend against criminal activity.
I  OVERVIEW

The Russian legal system is based on a continental civil law, code-based system. Both federal and regional legislation exist; however, federal legislation takes priority in cases of conflict. Generally, the issues of data privacy are regulated at federal level, and the regions of Russia do not issue any specific laws or regulations in this respect.

The latest Constitution of Russia, which provides that each individual has a right to privacy and personal and family secrets, was adopted in 1993. Each individual has a right to keep his or her communication secret, and restriction of this right is allowed only subject to a court decision. Collection, storage, use and dissemination of information about an individual’s private life are allowed only with the individual’s consent. The protection of these basic rights is regulated by special laws (e.g., on communications) and also specific regulations enacted in relation to these laws.

In 2007, Russia adopted a major law regulating data privacy issues, Federal Law No. 152-FZ on Personal Data dated 27 July 2006 (the Personal Data Law). The Personal Data Law covers almost all aspects of data protection, for example, what is considered personal data, what types of data can be collected and processed, how and in what cases data can be collected and processed, and what technical and organisational measures must be applied by companies or individuals that collect data. Unlike European law, the Personal Data Law does not distinguish between data controllers and data processors. Therefore, any individual or entity working with personal data is considered a personal data operator and thus falls under the regulation of the Personal Data Law. There are also several specific regulations, mainly covering the technical side of data processing and to a certain extent clarifying the provisions of the Personal Data Law. Such regulations are issued by the Russian government, the Russian data protection authority (i.e., the Federal Service for Supervision in the Sphere of Communication, Information Technology and Mass Communications (DPA)) or the authorities responsible for various security issues in Russia, such as the Federal Service for Technical and Export Control (FSTEK) or the Federal Security Service (FSB).

Since 2007, data privacy has never been a topic of intense discussion or major enforcement. However, this changed rather dramatically in 2014. The general approach of the government to privacy became fairly protectionist. Even though the officials usually make statements to the media that free data flows and the development of worldwide interconnected technologies is the real present and they do not want to impede the development of technologies, in reality the new laws adopted during the last four years are creating artificial barriers and
thus harming Russian business. In 2014, the Russian parliament adopted amendments to the Personal Data Law (that then became known as the Data Localisation Law) that require data operators that collect Russian citizens’ personal data to store and process such personal data using databases located in Russia. The Data Localisation Law was highly criticised by business and the media but nevertheless came into force on 1 September 2015. While this law generated a great deal of profit for Russian data centres, it also created high costs for ordinary businesses, which needed to redesign their data storage infrastructure.

In addition to the Data Localisation Law, Russia adopted amendments to the Russian Federal Law on Information, Information Technology and Protection of Information. These amendments require companies that provide video, audio or text communication services (usually ‘messengers’) to register with the authorities, to store users’ messages or audio or video calls for up to six months and to provide the security authorities with decryption keys if the messages are encrypted. These rules have resulted in the blocking of Blackberry Messenger and a few other messengers in Russia and in a campaign to block the Telegram messenger.

II THE YEAR IN REVIEW

Recent years have been very intense for Russian data protection law. The first step was Federal Law No. 97-FZ of 5 May 2014, which significantly amended Federal Law No. 149-FZ dated 27 July 2006 on Information, Information Technologies and Protection of Information (the Information Law) and some other Russian regulations. The Information Law was later substantially strengthened with a few additional amendments finally coming into force on 1 July 2018. Authored by conservative lawmaker Irina Yarovaya and nicknamed by Edward Snowden the ‘Big Brother law’, the amendments (the Yarovaya Law) will also directly affect Russia’s telecom and internet industries. In particular, mobile operators will need to store the recordings of all phone calls and the content of all text messages for a period of six months, entailing huge costs, while internet companies (e.g., messengers) need to store the recordings of all phone calls and the content of all text messages for six months and the related metadata for one year.

In addition, the Yarovaya Law requires such operators to provide any such communications to Russian police and intelligence at their request and to install special systems used for investigation purposes or ‘reconcile the use of software and hardware with the authorities’ as well as to provide the security authorities with decryption keys if the messages are encrypted.

Non-compliance may result in fines or blocked access to the non-compliant service. The parts of Yarovaya Law that are already effective are actively enforced by the DPA, and several messengers, including Blackberry Messenger, Imo and Vchat, have been blocked in Russia. In May 2017, the DPA also blocked WeChat and unblocked it once it had registered with the DPA. The relevant enforcement also resulted in a major case against Telegram messenger described in more detail below.

As a second step in data protection-related legislation, the Russian authorities adopted the Data Localisation Law and created a new procedure restricting access to websites that violate Russian laws on personal data.

In particular, based on the Data Localisation Law, the DPA created a register of infringing websites. The law provides for a detailed ‘notice and take down’ procedure. Most
importantly, the Data Localisation Law requires that all personal data of Russian citizens must be stored and processed in Russia. The location of databases with personal data of Russian citizens must be reported to the DPA.

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

According to the Personal Data Law ‘personal data’ means any information referring directly or indirectly to a particular individual or which can be used to verify an individual identity. The law does not specifically define any types of sensitive data, but lists special categories of personal data such as ‘race; nationality; political, religious, or philosophical views; health; and private life’. The purpose of the Personal Data Law is to regulate the processing of personal data by state authorities, private entities and individuals. Thus, the law establishes the rights of individuals, and sets out the obligations for legal and natural persons when processing personal data.

Any individual or company that collects and processes personal data is considered a personal data operator and thus is subject to the regulations of the Personal Data Law and state control. The Personal Data Law and other related regulations do not make any distinction between data controllers and data processors. Therefore, the law applies in its entirety to anyone dealing with personal data except where explicitly provided otherwise in the Personal Data Law.

There are also several specific regulations that primarily cover the technical side of data processing and to a certain extent clarify the provisions of the Personal Data Law. Among such regulations are Decree No. 1119 of the government of Russia (dated 1 January 2012 and enacted pursuant to Article 19 of the Personal Data Law) (Decree No. 1119). Decree No. 1119 provides for four general levels of protection to be applied by personal data operators depending on the quantity and types of data processed in the information systems. The detailed technical requirements placed on personal data processing are defined by FSTEK.

Although there has been steady growth in monitoring and the DPA is working more and more actively, the overall level of compliance with the Personal Data Law still appears to be low in Russia for various reasons, including (1) low fines; (2) slow work by the DPA; and (3) ambiguous provisions of the Personal Data Law that make compliance difficult.

ii General obligations for data handlers

Certain organisational and technical steps need to be taken to ensure compliance with the Personal Data Law. Data handlers must:

a collect the consent of personal data subjects: consent is required to be collected and in certain cases be in writing (ink on paper) unless certain exemptions are clearly applicable;

b check the country of the data recipient: in the event of cross-border transfers, the transferring entity needs to check whether the country of the data recipient is deemed to provide adequate protection to personal data, since if not, the consent needs to be in writing and contain a specific authorisation to transfer personal data to such country.

c have a data transfer agreement: the Personal Data Law requires that the transferring entity and the data recipient enter into an agreement that must stipulate that the data recipient will ensure at least the same level of data protection as applied by the transferring entity;
have a primary database in Russia: it must be ensured that the primary database with the personal data of any Russian citizens is located in Russia (e.g., in a Russian data centre or on any other server);

- comply with technical requirements: data operators must ensure that their systems are compliant with the technical requirements of the FSB and FSTEK, as well as Decree No. 1119;

- perform a data protection audit: every three years, data operators must perform an internal data protection audit and as a result of such audit adopt a document confirming that the data protection processes are in compliance with the Personal Data Law;

- adopt internal regulations on personal data protection and a privacy policy: if the data is collected online, the privacy policy must be published on the operator's website and in the mobile app where the users need to consent to such policy;

- appoint a data privacy officer (i.e., an employee who will be in charge of implementation and control of clients’ personal data protection);

- handle requests of individuals: data operators must comply with the requests of individuals related to their personal data. Such requests must be answered (e.g., access to personal data granted; personal data deleted at the request of the individual, etc.);

- define potential threats to personal data subjects: data operators must adopt an internal document that assesses the potential threat to data subjects in the event of, for example, unauthorised disclosure of their personal data and what measures are implemented in order to avoid damage to data subjects;

- acquaint its employees with the internal data protection processes and regulations, and conduct training sessions on personal data security; and

- register with the DPA (unless subject to exemptions).

The above list of steps is rather standard and may apply to most data operators; however, it is not exhaustive and the relevant measures may vary depending on the types of data collected and the means of collection and processing. The exact list of measures must be defined on a case-by-case basis.

### iii Specific regulatory areas

The Personal Data Law applies to all types of operators and data subjects. However, certain industry-specific aspects should also be noted. The Central Bank of Russia represents itself as a super regulator, for instance, requiring banks to report cybersecurity incidents.

Russian labour laws require employers to obtain the written consent of employees to transfer their personal data to third parties, for instance when such transfer is necessary to share data with group companies. However, when the employer has a legitimate interest or when required by law, the transfer can be made without such consent.

Protection of children and their privacy as well as financial, health and communications privacy are also regulated by specific laws, such as the Federal Law on Communication. However, the rules contained in these laws are mostly declarative, requiring the protection of the privacy and confidentiality of communications data, prohibiting mention of the names of children who have been the victims of criminal actions in mass media, etc.

### iii Technological innovation

Developments in Russian privacy legislation and Personal Data Law used to be very slow, and they obviously do not yet meet the demands of the rapid changes in technological
innovation. Issues such as location tracking, Big Data, data portability, employee monitoring, facial recognition technology, behavioural advertising and electronic marketing remain, to a certain extent, grey areas without adequate regulation.

However, the situation is changing. For instance, the DPA and the courts currently support the idea that technological measures such as cookies constitute personal data. This definitely makes business operations even more complicated. In addition, the lawmakers intend to adopt a law on big data with a potential requirement to localize all data in Russia.

IV INTERNATIONAL DATA TRANSFER AND DATA LOCALISATION

International data transfers in Russia are regulated by the Personal Data Law. The Personal Data Law distinguishes between countries that provide adequate protection for personal data and those that do not. In the event of cross-border transfers, a data operator needs to check whether the country of the data recipient is deemed a provider of adequate protection to personal data, since if not, the consent of the data subject needs to be in writing (ink on paper) and contain a specific authorisation to transfer personal data to such country. The Personal Data Law provides for only three categories of lawful cross-border transfer of Personal Data:

a. transfer to countries that are signatories to the Council of Europe Convention 1981 (the Personal Data Convention);

b. transfer to countries that are not signatories to the Personal Data Convention but are on the list of additional countries adopted by the DPA. The current version of the list (as amended on 15 June 2017) includes Angola, Argentina, Australia, Benin, Canada, Cape Verde, Chile, Costa Rica, Gabon, Israel, Kazakhstan, Malaysia, Mali, Mexico, Mongolia, Morocco, New Zealand, Peru, Qatar, Singapore, South Africa, South Korea and Tunisia; and

c. transfers to any other countries (e.g., the United States) that are neither on the list of additional countries nor signatories to the Personal Data Convention, provided that there is explicit handwritten (ink on paper) consent of the data subject to such transfer.

Obtaining written consent is in many cases a core element of Russian data protection law. However, this may become a burdensome procedure, especially for companies that do business on the internet. The main problem is that the only alternative to a wet signature is a qualified enhanced electronic signature. Under Russian law, only a qualified enhanced e-signature has the legal force of a handwritten signature. Such signatures must be created using certified encryption software and are obtained at special certification centres. It is very uncommon for an individual to have this tool.

The Personal Data Law also requires that the data exporter and the data importer enter into an agreement (or at least add a provision to their agreement in the event of a cross-border transaction) that must stipulate that the data importer will ensure at least the same level of data protection as applied by the data exporter and certain other obligations provided under the Personal Data Law.

V COMPANY POLICIES AND PRACTICES

All companies must ensure that their internal employee policies address personal data protection and that they have general internal policies on data protection and organisational
and technical measures to be taken by the company in order to protect personal data. Normally, all of the above can be covered in a single privacy policy. However, in practice not all companies have implemented privacy policies, especially small and mid-sized companies.

Russian laws on trade unions give trade unions powers to influence labour-related decisions, for example, certain decisions affecting labour relations. The company must take into account the opinion of the trade union in cases provided for by law, such as regulatory acts, internal regulations (local normative acts), or collective agreements. Thus, before the approval and implementation of the privacy policy, the opinion of the trade union must be requested.

As already noted above, all companies must appoint an internal data privacy officer. The Personal Data Law does not provide much detail with respect to data privacy officers, their role in the company and detailed regulation of their rights. Therefore, these are normally covered in privacy policies as well.

Companies are obliged to have internal documents covering various aspects of information security, including technical and organisational measures to be taken by the companies. Normally, such documents are developed by external service providers that have a state licence to provide information security services. These documents are of a technical nature and normally cover the types of software and hardware a company should use to protect its information systems that contain personal data.

VI DISCOVERY AND DISCLOSURE

Generally, Russian law presumes a high degree of cooperation with state authorities in the event of investigations conducted by state authorities. Disclosure of data (including personal data) is required under various statutes, so that a business is required to provide data to state authorities upon their request, which must be based on a statute. For instance, the provision of personal data to the police for criminal investigations must be based on the request by the police that must comply with Russian laws on operative investigation activities. Normally, the disclosure request must be approved by a court; however, Russian courts are very cooperative with investigation authorities; therefore, the possibilities to refuse to disclose the data to the authorities are very limited.

The degree to which the authorities expect cooperation on data disclosure was evident in the example mentioned in Section II above, the Yarovaya Law. This law provides that organisers of internet messaging must provide the message data to the authorities and the authorities are even entitled to require that organisers install special systems used for investigation purposes.

It is very difficult, and in most cases even prohibited, to disclose data in response to requests from foreign governments. The data can be provided on the basis of international treaties on legal assistance between the countries. However, in this case, a foreign government agency should request the data through the Russian authorities.

There is still a possibility to disclose data directly with the data subjects’ written consent; however, this could become very problematic from a practical perspective.
VII  PUBLIC AND PRIVATE ENFORCEMENT

i  Enforcement agencies

The primary agency dealing with personal data breaches is the DPA. The DPA is entitled to perform scheduled and unscheduled audits. The schedule of all planned compliance audits for the next year is usually published on the websites of the territorial subdivisions of the DPA. However, the DPA can also perform unscheduled checks and is required to notify the individual or company at least 24 hours before the check.

The DPA performs its own monitoring of data breaches (including monitoring of the internet and the relevant news). The DPA also quite actively reacts to complaints, which in practice can be filed by data subjects, prosecutors or competitors. Following a complaint or based on the results of its own monitoring, the DPA performs a non-scheduled check, informing the company 24 hours before.

As a result of such a check, the DPA can issue an order to resolve the breach or institute administrative proceedings in a local court. Based on the statistics, the DPA does not initiate proceedings very frequently. This means that in most cases breaches can be resolved based on the DPA’s order.

Data operators may be subject to criminal, civil and administrative liability. The individuals whose personal data has been compromised have a private right to sue, with the right to demand compensation for losses or compensation for ‘moral harm’.

The DPA is entitled to initiate administrative proceedings in the event of a data breach and impose administrative sanctions (fines) if the breach is proven. In addition, the DPA may, subject to a court decision, block infringing websites or mobile applications from being accessed in Russia.

The current maximum administrative fine is 75,000 roubles. In practice, the administrative fines are not multiplied by, for example, the number of emails or employees whose data was compromised or by the number of specific data breaches, but instead applied only once for a particular type of breach. However, this practice may change in the near future.

Criminal sanctions can be applied only against natural persons and can never be applied against companies. However, even those Articles of the Russian Criminal Code that could theoretically apply to personal data breaches are never applied to such cases as far as we know.

ii  Recent enforcement cases

The Data Localisation Law was hardly enforced for some time. However, in 2016, a major case involving LinkedIn attracted a great deal of attention from the public. A Russian district court upheld a claim by the DPA seeking restriction of access to LinkedIn in Russian territory. The judgment was handed down on 4 August 2016. The information on the case, however, was not disclosed to the media until 25 October 2016.

The court found LinkedIn to be liable of a violation of the Personal Data Law, in particular of its provisions requiring Russian citizens’ personal data to be stored and processed on servers located in Russia. The court found that LinkedIn does not operate a server in Russia. Furthermore, in the court’s view, LinkedIn processed the personal data of third parties who were not covered by a user agreement. On this basis, the court declared LinkedIn to be in violation of the Personal Data Law and ordered the DPA to take steps to restrict access to LinkedIn. Currently, LinkedIn still remains blocked in Russia.
The same lack of enforcement accompanied the Yarovaya Law. There were occasional blockings (such as Blackberry Messenger); however, due to the limited popularity of such messaging services, the enforcement cases did not attract much attention. Everything changed with a case regarding one of the most popular messengers in Russia – Telegram. On 20 March 2018, the Supreme Court of Russia dismissed the claim by a representative of the Telegram messaging service to abolish the order of FSB dated 19 July 2016 requiring messaging services to provide decryption keys to the FSB, which allow the security authorities to read correspondence by Telegram’s users.

Telegram has frequently commented in the press that it is unable to provide the decryption keys due to the nature of end-to-end encryption technology, while the FSB believes this is technically possible. Telegram finally refused to provide the FSB with any decryption keys and, therefore, on 13 April 2018, the Taganskyi District Court of Moscow upheld the DPA’s claim to block access to Telegram. On 16 April 2018, the DPA reached out to telecom operators, requesting that they commence blocking the messenger. All Russian telecom operators are obliged to block access to the relevant resources.

Telegram’s lawyers appealed this decision without success. Since April 2018, the DPA has been trying to block Telegram using its IP address, which seems to be an ineffectual strategy. Telegram decided to contend with the DPA (luckily they have no actual presence in Russia) and started jumping from one IP address to another. At one time, the DPA was blocking millions of IP addresses, which caused interruptions in many internet services (including those hosted on the Amazon and Google networks) and caused negative criticism of the DPA by other authorities, the internet ombudsman and businesses. There was at least one court case where a company that suffered from blocking (even though they are not related to Telegram) sued the DPA. The case is to be tried this year. So far, the chase continues and Telegram is still available despite the DPA’s actions.

iii Private litigation

The individuals whose personal data is processed in a manner not in compliance with the Personal Data Law are entitled to claim damages or compensation for moral harm from the infringing company. Such claims can only be adjudicated in a court trial between the affected data subject and the infringer. Generally, the cases where the data subjects use this option (i.e., raise such compensation or damage claims before courts) are fairly rare, and it is unlikely that the number of civil law lawsuits will increase in the near future. The main reason for this is that claimants must go through the cumbersome court procedure and provide evidence of the damage (including moral harm) caused to them. In addition, the competent Russian courts do not award large sums for the data breaches (usually only a few thousand roubles). In practice, individuals prefer submitting complaints to the DPA or the Russian prosecutor’s office, which can initiate a compliance audit of the infringing entity by the DPA.

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

Having a representative office in Russia or even working through a Russian subsidiary automatically triggers the necessity of compliance with Russian data protection regulations. Sometimes the DPA attempts to interpret Russian data protection laws as having jurisdiction over foreign companies. Requests by the DPA to foreign companies to provide internal documents on personal data compliance and give explanations on the alleged data breaches are not unusual. However, in the absence of any substantial cooperation between the DPA and
foreign data protection authorities as well as the lack of relevant treaties on legal assistance, the prospects of enforcement against a purely foreign legal entity are doubtful. In any event, the issues described in this chapter, in particular data-localisation requirements, must be taken into consideration by any foreign companies intending to expand their business to the Russian market. The LinkedIn case also confirms that even the lack of a presence in Russia does not release foreign data operators from the obligation to comply with certain requirements of the Personal Data Law.

IX CYBERSECURITY AND DATA BREACHES

The topic of cybersecurity is becoming more and more important in Russian discussions. The first issues that come to mind are certainly the alleged Russian hacking of the US presidential elections. The US media reported that the US administration was contemplating an unprecedented covert cyber action against Russia in retaliation for alleged Russian interference in the American presidential election. At least according to the media, the CIA has been asked to deliver options to the White House for a cyber-operation designed to harass and ‘embarrass’ the Kremlin leadership.

Another infamous cybersecurity issue was the ransomware attacks WannaCry and Petrwrap/Petya. Major Russian and Western companies working in Russia were paralysed by the attacks for several days.

All these security issues have prompted calls for Russia’s internet infrastructure to be protected. As a consequence, on 26 July 2017, Russia adopted Federal Law No. 187-FZ on the Security of Critical Information Infrastructure of the Russian Federation. The law sets out the basic principles for ensuring the security of critical information infrastructure, the powers of the state bodies of Russia to ensure the security of the critical information infrastructure, as well as the rights, obligations and responsibilities of persons holding rights of ownership or other legal rights to the facilities for critical information infrastructure, communications providers and information systems providing interaction with these facilities.

The elements of the critical information infrastructure are understood to be information systems, telecommunication networks of state authorities as well as such systems and networks for the management of technological processes that are used in state defence, healthcare, transport, communication, finance, energy, fuel, nuclear, aerospace, mining, metalworking and chemical industries. All these industries are considered critical for the economy and should be protected against any cyberthreats. The law requires such industries to implement protection measures, assign the category of protection (in accordance with the statutes) and then register with FSTEK, which is now the supervisory authority in this field. So far, businesses have many questions to the authorities with respect to this law, which is very broadly drafted. The usual question is whether the law applies to a particular business or not, since even internal LAN networks may be considered critical information infrastructure under such general rules of the law. However, the authorities usually reply that this is an incorrect interpretation. The lack of enforcement practice does not help to clarify the situation.

The potential abuse of information systems for illicit purposes poses new security risks to the government and to businesses. As a result, Russian authorities have introduced rules requiring foreign software producers to allow the agencies certified by Russian state authorities to review the source code of the software (in most cases security products such as
firewalls, anti-virus applications and software containing encryption) before permitting the products to be imported and sold in the country. This is done to ensure that there are no ‘backdoors’ in the software that could be used by foreign intelligence services.

X OUTLOOK

The major issues for the upcoming years are still the Data Localisation Law and Yarovaya Law. Generally, there is a strong feeling that Russian data protection law and internet regulations as such will move towards more formalisation and less room for flexibility because the authorities welcome additional control over the internet and personal data flows.

Furthermore, there are various initiatives related to regulation of Big Data, various comparatively minor amendments to the Personal Data Law (e.g., new fines for failure to ensure proper data processing by data recipients under data transfer agreements), etc.

It is also expected that more court practice will appear. The number of court cases related to data privacy is already increasing and we expect even more enforcement actions and court clarifications in this field.
Chapter 21

SINGAPORE

Yuet Ming Tham

I  OVERVIEW

In 2017 and 2018, Singapore has continued to rapidly develop its data protection, cybercrime, and cybersecurity regimes. As set out in Singapore’s October 2016 cybersecurity strategy report, the government views its efforts in these areas as part of an integrated cybersecurity plan to protect the country from cyberthreats and to reinforce Singapore’s standing as a leading information systems hub. The key legal components in this strategy include the Personal Data Protection Act 2012 (PDPA), Singapore’s first comprehensive framework established to ensure the protection of personal data, the Computer Misuse and Cybersecurity Act (CMCA) to combat cybercrime and other cyberthreats, and the recently passed Cybersecurity Act (the Cybersecurity Act), which focuses on protecting Singapore’s critical information infrastructure (CII) and establishing a comprehensive national cybersecurity framework.

In this chapter, we will outline the key aspects of the PDPA, CMCA and the Cybersecurity Act. The chapter will place particular emphasis on the PDPA, including a brief discussion of the key concepts, the obligations imposed on data handlers, and the interplay between technology and the PDPA. Specific regulatory areas such as the protection of minors, financial institutions, employees and electronic marketing will also be considered. International data transfer is particularly pertinent in the increasingly connected world; how Singapore navigates between practical considerations and protection of the data will be briefly examined. We also consider the enforcement of the PDPA in the event of non-compliance.

This chapter also will review the amendments to the CMCA and the CMCA’s linkages with the Cybersecurity Act. The discussion will cover the proposed consolidation of cybersecurity authority within Singapore’s Cybersecurity Agency (CSA) and the new position of Commissioner of Cybersecurity established by the Cybersecurity Act.

II  THE YEAR IN REVIEW

i  PDPA developments

There were a number of significant developments related to the PDPA and the Personal Data Protection Commission (PDPC) – the body set up to administer and enforce the PDPA – in the 12 months from September 2017 to August 2018. In July 2017, the PDPC had initiated a public consultation to consider proposed changes to the PDPA that would have the effect of

1 Yuet Ming Tham is a partner at Sidley Austin LLP.
broadening the circumstances under which organisations could collect, use and disclose personal data without consent, and (2) imposing a mandatory data breach notification requirement in certain situations. The consultation period closed on 5 October 2017, and the PDPC issued its responses to the feedback on 1 February 2018.3 Regarding consent, the PDPC had proposed not requiring consent if it would be impractical for the organisation to obtain consent and the collection, use and disclosure of the personal data were not expected in any way to have an adverse effect on the individual. In such a situation, the PDPC proposed allowing a notification-of-purpose in lieu of consent. In response to public feedback, the PDPC decided to remove the condition of ‘impractical to obtain consent.’ The PDPC also proposed creating a catch-all ‘legal or business purpose’ exception to consent where it would not be desirable or appropriate to obtain the individual’s consent and the benefits to the public generally or to a subset of the public ‘clearly outweigh’ any adverse effect or risks to the individual (such as where an organisation would like to share personal data in order to detect and prevent fraudulent activity). Following public feedback, the PDPC proposed to instead provide for a ‘legitimate interests’ exception to consent, which would be an evolution of the ‘legal or business purpose’ approach and would be further clarified in future guidelines from the PDPC. Regarding the data breach notification requirement, the PDPC had proposed to require data breach notification in the following circumstances: (1) if there is any risk of impact or harm to affected individuals, the organisation must notify the individuals and the PDPC; (2) if the scale of the data breach is ‘significant’ (i.e., involving 500 or more individuals), the organisation must notify the PDPC; and (3) if a data intermediary experiences a breach, it must notify its clients immediately. In response to public feedback, the PDPC announced that it will not prescribe a statutory threshold for the number of affected individuals (i.e., 500) that would constitute a ‘significant’ data breach, but rather would issue guidance on assessing the scale of impact.

In March 2018, Singapore announced that it had joined the Asia-Pacific Economic Cooperation (APAC) Cross-Border Privacy Rules (CBPR) system, as well as the APAC Privacy Recognition for Processors (PRP) programme. Upon joining, Singapore became the sixth member of the CBPR system – which already included Canada, Japan, Korea, Mexico and the United States – and the second member of the PRP programme after the United States. APEC established the CBPR programme to facilitate the transmittal of personal data across national borders within and between companies and organisations. (The APEC PRP programme seeks to accomplish similar goals for data processors.) Companies and organisations in CBPR member countries that collect and use personal data may obtain CBPR certification through a compliance review process by an independent evaluator. The Singapore government has indicated that the PDPC intends to launch a certification scheme for both the CBPR and PRP standards by the end of 2018.

In April 2018, the PDPC issued a Public Consultation for Managing Unsolicited Commercial Messages and the Provision of Guidance to Support Innovation in the Digital Economy. This consultation aims to bring together and streamline existing ‘do not call’ rules contained in the PDPA and the Spam Control Act, ban parties from screening the do not call registry and selling the resulting information to marketers, and include instant messages within the remit of the PDPA. This consultation closed on 12 June 2018.

ii  CMCA developments and the Cybersecurity Act

The CMCA and the Cybersecurity Act are closely linked. In the October 2016 Cybersecurity Report, the government noted the need for a comprehensive framework to prevent and manage the increasingly sophisticated threats to Singapore’s cybersecurity. According to the report, the Cybersecurity Act would establish that framework and would complement the existing cybercrime measures set out in the CMCA.

In 2013, the government amended the existing Computer Misuse Act, renaming it the Computer Misuse and Cybersecurity Act, to strengthen the country’s response to national-level cyberthreats. In 2017, the government introduced further amendments to the CMCA, and the amended law came into effect on 1 June 2017. The amendments broadened the scope of the CMCA by criminalising certain conduct not already covered by the existing law and enhancing penalties in certain situations. For example, the new provisions of the CMCA criminalise the use of stolen data to carry out a crime even if the offender did not steal the data himself or herself, and prohibits the use of programs or devices used to facilitate computer crimes, such as malware or code crackers. The amendments also extended the extraterritorial reach of the CMCA by covering actions by persons targeting systems that result in, or create a significant risk of, serious harm in Singapore, even if the persons and systems are both located outside Singapore.

In keeping with the government’s emphasis on safeguarding critical information infrastructure, on 5 February 2018, Singapore passed the Cybersecurity Bill No. 2/2018 (the Cybersecurity Act), a draft of which had previously been issued for public consultation on 10 July 2017. The Cybersecurity Act addresses the regulation of CII, creates a new Commissioner of Cybersecurity with significant powers to prevent and respond to cybersecurity incidents in Singapore, and sets up a licensing scheme for providers of certain cybersecurity services.

CII is defined as computer systems, located at least partly within Singapore, that are necessary for the continuous delivery of an essential service such that the loss of a system would have a debilitating effect on the availability of the essential service in Singapore. The Commissioner will designate those systems that it determines qualify as CII, and will notify the legal owner of such systems in writing. An owner or operator of a system that has been designated as CII must comply with various requirements set forth in the Act, including reporting to the Commissioner certain prescribed incidents, establishing mechanisms and processes for detecting cybersecurity threats and incidents, and reporting any material changes to the design, configuration, security or operation of the CII.

Under the Cybersecurity Act, the Commissioner’s authority goes beyond CII, however. Any organisation, even if it does not own or operate CII, must cooperate with the Commissioner in the investigation of cybersecurity threats and incidents. In furtherance of such investigations, the Commissioner may, among other things, require any person to produce any physical or electronic record or document, and require an organisation to carry out such remedial measures or cease carrying out such activities as the Commissioner may direct.

Finally, the Act establishes a licensing regime for providers of (1) services that monitor the cybersecurity levels of other persons’ computers or systems, and (2) services that assess, test or evaluate the cybersecurity level of other persons’ computers or systems by searching for vulnerabilities in, and compromising, the defences of such systems. Any person who provides
a licensable cybersecurity service without a licence will be guilty of an offence. According to the Cybersecurity Agency’s ‘Cybersecurity FAQs’, the licensing framework is expected to be implemented in the second half of 2019.4

iii 2018 Developments and regulatory compliance

Although the developments with the CMCA and the Cybersecurity Act represent significant milestones in Singapore’s overall cybersecurity strategy, the key compliance framework from the perspective of companies and organisations remains at this point with data protection and privacy. The CMCA is primarily a criminal statute, and the government has not issued any regulations or guidelines for the CMCA. The Cybersecurity Act imposes a number of legal requirements on CII owners and cybersecurity service providers, but until the government issues implementing regulations or advisory guidance regarding these new requirements, organisations’ focus will be on the PDPA and its related regulations, subsidiary legislation and advisory guidelines.5

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

The PDPA framework is built around the concepts of consent, purpose and reasonableness. The main concept may be summarised as follows: organisations may collect, use or disclose personal data only with the individual’s knowledge and consent (subject to certain exceptions) for a purpose that would be considered appropriate to a reasonable person in the circumstances.

There is no prescribed list of ‘personal data’; rather, these are defined broadly as data about an individual, whether or not they are true, who can be identified from that data or in conjunction with other information to which the organisation has or is likely to have access.6 In addition, the PDPA does not distinguish between personal data in its different forms or media. Thus, there is no distinction made for personal data that are ‘sensitive’, or between data that are in electronic or hard copy formats. There are also no ownership rights conferred on personal data to individuals or organisations.7 There are certain exceptions to which the PDPA would apply. Business contact information of an individual generally falls outside the ambit of the PDPA,8 as does personal data that is publicly available.9 In addition, personal data of an individual who has been deceased for over 10 years10 and personal data contained within records for over 100 years is exempt.11

---

5 Government agencies are not covered by the scope of the PDPA.
6 Section 2 of the PDPA.
7 Section 5.30, PDPA Key Concepts Guidelines.
8 Section 4(5) of the PDPA.
9 Second Schedule Paragraph 1(c); Third Schedule Paragraph 1(c); Fourth Schedule Paragraph 1(d) of the PDPA.
10 Section 4(4)(b) of the PDPA. The protection of personal data of individuals deceased for less than 10 years is limited; only obligations relating to disclosure and protection (Section 24) continue to apply.
11 Section 4(4) of the PDPA.
Pursuant to the PDPA, organisations are responsible for personal data in their possession or under their control. 12 ‘Organisations’ include individuals who are resident in Singapore, local and foreign companies, associations and bodies (incorporated and unincorporated), whether or not they have an office or a place of business in Singapore. 13 The PDPA does not apply to public agencies. 14 Individuals acting in a personal or domestic capacity, or where they are an employee acting in the course of employment within an organisation, are similarly excluded from the obligations imposed by the PDPA. 15

Where an organisation acts in the capacity of a data intermediary, namely an organisation that processes data on another’s behalf, it would only be subject to the protection and retention obligations under the PDPA. The organisation that engaged its services remains fully responsible in respect of the data as if it had processed the data on its own. 16

There is no requirement to prove harm or injury to establish an offence under the PDPA, although this would be necessary in calculating damages or any other relief to be awarded to the individual in a private civil action against the non-compliant organisation. 17

Subsidiary legislation to the PDPA includes implementing regulations relating to the Do Not Call (DNC) Registry, 18 enforcement, 19 composition of offences, 20 requests for access to and correction of personal data, and the transfer of personal data outside Singapore. 21 There is also various sector-specific legislation, such as the Banking Act, the Telecommunications Act and the Private Hospitals and Medical Clinics Act, imposing specific data protection obligations. All organisations will have to comply with PDPA requirements in addition to the existing sector-specific requirements. In the event of any inconsistencies, the provisions of other laws will prevail. 22

The PDPC has released various advisory guidelines, as well as sector-specific advisory guidelines for the telecommunications, real estate agency, education, social services and healthcare sectors. The PDPC has also published advisory guidelines on data protection relating to specific topics such as photography, analytics and research, data activities relating to minors and employment. While the advisory guidelines are not legally binding, they provide helpful insight and guidance into problems particular to each sector or area.

ii General obligations for data handlers

The PDPA sets out nine key obligations in relation to how organisations collect, use and disclose personal data, as briefly described below.

---

12 Section 11(2) of the PDPA.
13 Section 2 of the PDPA.
14 Section 4(1)(c) of the PDPA.
15 Section 4(1)(a) and (b) of the PDPA.
16 Section 4(3) of the PDPA.
17 Section 32 of the PDPA.
18 Personal Data Protection (Do Not Call Registry) Regulations 2013.
19 Personal Data Protection (Enforcement) Regulations 2014.
20 Personal Data Protection (Composition of Offences) Regulations 2013.
21 Personal Data Protection Regulations 2014.
22 Section 6 of the PDPA.
Consent
An organisation may only collect, use or disclose personal data for purposes to which an individual has consented. Where the individual provided the information voluntarily and it was reasonable in the circumstances, the consent may be presumed. Consent may be withdrawn at any time with reasonable notice. The provision of a service or product must not be made conditional upon the provision of consent beyond what is reasonable to provide that product or service.

An organisation may obtain personal data with the consent of the individual from a third party source under certain circumstances. For example, with organisations that operate in a group structure, it is possible for one organisation in the group to obtain consent to the collection, use and disclosure of an individual’s personal data for the purposes of the other organisations within the corporate group.

Purpose limitation
Organisations are limited to collecting, using or disclosing personal data for purposes that a reasonable person would consider appropriate in the circumstances and for a purpose to which the individual has consented.

Notification
Organisations are obliged to notify individuals of their purposes for the collection, use and disclosure of the personal data on or before the collection, use and disclosure. The PDPC has also released a guide to notification to assist organisations in providing clearer notifications to consumers on the collection, use and disclosure of personal data that includes suggestions on the layout, language and placement of notifications.

Access and correction
Save for certain exceptions, an organisation must, upon request, provide the individual with his or her personal data that the organisation has in its possession or control, and how the said personal data has been or may have been used or disclosed by the organisation during the past year. The organisation may charge a reasonable fee in responding to the access request.

The organisation is also obliged to allow an individual to correct an error or omission in his or her personal data upon request, unless the organisation is satisfied that there are reasonable grounds to deny such a request.

23 Sections 13 to 17 of the PDPA.
24 In Section 12.42 of the PDPA Key Concepts Guidelines, the PDPA would consider a withdrawal notice of at least 10 business days from the day on which the organisation receives the withdrawal notice to be reasonable notice. Should an organisation require more time to give effect to a withdrawal notice, it is good practice for the organisation to inform the individual of the time frame under which the withdrawal of consent will take effect.
25 Section 12.32, PDPA Key Concepts Guidelines.
26 Section 18 of the PDPA.
27 Section 20 of the PDPA.
29 Sections 21 and 22 of the PDPA.
30 Section 22(6) and Sixth Schedule of the PDPA.
An organisation should respond to an access or correction request within 30 days, beyond which the organisation should inform the individual in writing of the time frame in which it is able to provide a response to the request.\textsuperscript{31}

**Accuracy**\textsuperscript{32}
An organisation is obliged to make a reasonable effort to ensure that the personal data collected by or on behalf of the organisation are accurate and complete if they are likely to be used to make a decision that affects an individual or are likely to be disclosed to another organisation.

**Protection**\textsuperscript{33}
An organisation is obliged to implement reasonable and appropriate security safeguards to protect the personal data in its possession or under its control from unauthorised access or similar risks. As a matter of good practice, organisations are advised to design and organise their security arrangements in accordance with the nature and varying levels of sensitivity of the personal data.\textsuperscript{34}

**Retention limitation**\textsuperscript{35}
An organisation may not retain the personal data for longer than is reasonable for the purpose for which they were collected, and for no longer than is necessary in respect of its business or legal purpose. Beyond that retention period, organisations should either delete or anonymise their records.

**Transfer limitation**\textsuperscript{36}
An organisation may not transfer personal data to a country or territory outside Singapore unless it has taken appropriate steps to ensure that the data protection provisions will be complied with, and that the overseas recipient is able to provide a standard of protection that is comparable to the protection under the PDPA (see Section IV).

**Openness**\textsuperscript{37}
An organisation is obliged to implement necessary policies and procedures in compliance with the PDPA, and to ensure that this information is available publicly.

### iii Technological innovation and privacy law
The PDPC considers that an IP address or network identifier, such as an International Mobile Equipment Identity number, may not on its own be considered personal data as it simply

\textsuperscript{31} 15.18, PDPA Key Concepts Guidelines.
\textsuperscript{32} Section 23 of the PDPA.
\textsuperscript{33} Section 24 of the PDPA.
\textsuperscript{34} See discussion in Sections 17.1–17.3, PDPC Key Concepts Guidelines.
\textsuperscript{35} Section 25 of the PDPA.
\textsuperscript{36} Section 26 of the PDPA.
\textsuperscript{37} Sections 11 and 12 of the PDPA.
identifies a particular networked device. However, where IP addresses are combined with other information such as cookies, individuals may be identified via their IP addresses, which would thus be considered personal data.

In relation to organisations collecting data points tied to a specific IP address, for example, to determine the number of unique visitors to a website, the PDPC takes the view that if the individual is not identifiable from the data collected, then the information collected would not be considered personal data. If, on the other hand, an organisation tracks a particular IP address and profiles the websites visited for a period such that the individual becomes identifiable, then the organisation would be found to have collected personal data.

Depending on the purpose for the use of cookies, the PDPA would apply only where cookies collect, use or disclose personal data. Thus, in respect of session cookies that only collect and store technical data, consent is not required. Where cookies used for behavioural targeting involve the collection and use of personal data, the individual's consent is required. Express consent may not be necessary in all cases; consent may be reflected when an individual has configured his or her browser setting to accept certain cookies but reject others.

If an organisation wishes to use cloud-based solutions that involve the transfer of personal data to another country, consent of the individual may be obtained pursuant to the organisation providing a written summary of the extent to which the transferred personal data will be protected to a standard comparable with the PDPA. It is not clear how practicable this would be in practice; a cloud-computing service may adopt multi-tenancy and data commingling architecture to process data for multiple parties. That said, organisations may take various precautions such as opting for cloud providers with the ability to isolate and identify personal data for protection, and ensure they have established platforms with a robust security and governance framework.

As regards social media, one issue arises where personal data are disclosed on social networking platforms and become publicly available. As noted earlier, the collection, use and disclosure of publicly available data is exempt from the requirement to obtain consent. If, however, the individual changes his or her privacy settings so that the personal information is no longer publicly available, the PDPC has adopted the position that, as long as the personal data in question were publicly available at the point of collection, the organisation will be able to use and disclose the same without consent.

iv Specific regulatory areas

Minors

The PDPA does not contain special protection for minors (under 21 years of age). However, the Selected Topics Advisory Guidelines note that a minor of 13 years or older typically has sufficient understanding to provide consent on his or her own behalf. Where a minor is below the age of 13, an organisation should obtain consent from the minor's parents or legal
guardians on the minor’s behalf. The Education Guidelines provide further guidance on when educational institutions seeking to collect, use or disclose personal data of minors are required to obtain the consent of the parent or legal guardian of the student.

Given the heightened sensitivity surrounding the treatment of minors, the PDPC recommends that organisations ought to take relevant precautions on this issue. Such precautions may include making the terms and conditions easy to understand for minors, placing additional safeguards in respect of personal data of minors and, where feasible, anonymising their personal data before use or disclosure.

**Financial institutions**

A series of notices issued by the Monetary Authority of Singapore (MAS), the country’s central bank and financial regulatory authority, require various financial institutions to, among other things:

- upon request, provide access as soon as reasonably practicable to personal data in the possession or under the control of the financial institution, which relates to an individual’s factual identification data such as full name or alias, identification number, residential address, telephone number, date of birth and nationality; and
- correct an error or omission in relation to the categories of personal data set out above upon request by a customer if the financial institution is satisfied that the request is reasonable.

In addition, legislative changes to the Monetary Authority of Singapore Act, aimed at enhancing the effectiveness of the anti-money laundering and the countering of financing of terrorism (AML/CFT) regime of the financial industry in Singapore, came into force on 26 June 2015.

Following the changes, MAS has the power to share information on financial institutions with its foreign counterparts under their home jurisdiction on AML/CFT issues. MAS may also make AML/CFT supervisory enquiries on behalf of its foreign counterparts. Nonetheless, strong safeguards are in place to prevent abuse and ‘fishing expeditions’. In granting requests for information, MAS will only provide assistance for bona fide requests. Any information shared will be proportionate to the specified purpose, and the foreign AML/CFT authority has to undertake not to use the information for any purpose other than the specified purpose, and to maintain the confidentiality of any information obtained.

**Electronic marketing**

The PDPA contains provisions regarding the establishment of a national DNC Registry and obligations for organisations that send certain kinds of marketing messages to Singapore
telephone numbers to comply with these provisions. The PDPA Healthcare Guidelines\textsuperscript{46} provide further instructions on how the DNC provisions apply to that sector, particularly in relation to the marketing of drugs to patients. In relation to the DNC Registry, the obligations only apply to senders of messages or calls to Singapore numbers, and where the sender is in Singapore when the messages or calls are made, or where the recipient accesses them in Singapore. Where there is a failure to comply with the DNC provisions, fines of up to S$10,000 may be imposed for each offence.

**Employees**

The PDPC provides that organisations should inform employees of the purposes of the collection, use and disclosure of their personal data and obtain their consent.

Employers are not required to obtain employee consent in certain instances. For instance, the collection of employee’s personal data for the purpose of managing or terminating the employment relationship does not require the employee’s consent, although employers are still required to notify their employees of the purposes for their collection, use and disclosure.\textsuperscript{47} Examples of managing or terminating an employment relationship can include using the employee’s bank account details to issue salaries or monitoring how the employee uses company computer network resources. The PDPA does not prescribe the manner in which employees may be notified of the purposes of the use of their personal data; as such, organisations may decide to inform their employees of these purposes via employment contracts, handbooks or notices on the company intranet.

In addition, collection of employee personal data necessary for ‘evaluative purposes’, such as to determine the suitability of an individual for employment, neither requires the potential employee to consent to, nor to be notified of, their collection, use or disclosure.\textsuperscript{48} Other legal obligations, such as to protect confidential information of their employees, will nevertheless continue to apply.\textsuperscript{49}

Section 25 of the PDPA requires an organisation to cease to retain documents relating to the personal data of an employee once the retention is no longer necessary.

**IV  PDPA AND INTERNATIONAL DATA TRANSFER**

An organisation may only transfer personal data outside Singapore subject to requirements prescribed under the PDPA so as to ensure that the transferred personal data is afforded a standard of protection comparable to the PDPA.\textsuperscript{50}

An organisation may transfer personal data overseas if:

\begin{itemize}
  \item it has taken appropriate steps to ensure that it will comply with the data protection provisions while the personal data remains in its possession or control; and
\end{itemize}

\textsuperscript{46} Section 6 of the PDPC Healthcare Guidelines.

\textsuperscript{47} Paragraph 1(o) Second Schedule, Paragraph 1(j) Third Schedule, and Paragraph 1(s) Fourth Schedule of the PDPA.

\textsuperscript{48} Paragraph 1(f) Second Schedule, Paragraph 1(f) Third Schedule and Paragraph 1(h) Fourth Schedule of the PDPA.

\textsuperscript{49} Sections 5.14–5.16 of the PDPA Selected Topics Guidelines.

\textsuperscript{50} Section 26(1) of the PDPA. The conditions for the transfer of personal data overseas are specified within the Personal Data Protection Regulations 2014.
it has taken appropriate steps to ensure that the recipient is bound by legally enforceable obligations to protect the personal data in accordance with standards comparable to the PDPA. Such legally enforceable obligations would include any applicable laws of the country to which the personal data is transferred, contractual obligations or binding corporate rules for intra-company transfers.

Notwithstanding the above, an organisation is taken to have satisfied the latter requirement if, inter alia, the individual consents to the transfer pursuant to the organisation providing a summary in writing of the extent to which the personal data transferred to another country will be protected to a standard comparable to the PDPA; or where the transfer is necessary for the performance of a contract.

In respect of personal data that simply passes through servers in Singapore en route to an overseas destination, the transferring organisation will be deemed to have complied with the transfer limitation obligation.

The Key Concepts Guidelines also provide examples to illustrate situations in which organisations are deemed to have transferred personal data overseas in compliance with their transfer limitation obligation pursuant to Section 26 of the PDPA, regardless of whether the foreign jurisdiction’s privacy laws are comparable to the PDPA. An example is when a tour agency needs to share a customer’s details (e.g., his or her name and passport number) to make hotel and flight bookings. The tour agency is deemed to have complied with Section 26 since the transfer is necessary for the performance of the contract between the agency and the customer.

An organisation is also deemed to have complied with the transfer limitation obligation if the transfer is necessary for the performance of a contract between a Singaporean company and a foreign business, and the contract is one that a reasonable person would consider to be in the individual’s interest.

Other examples given by the Key Concepts Guidelines include the transferring of publicly available personal data, and transferring a patient’s medical records to another hospital where the disclosure is necessary to respond to a medical emergency.

The Key Concepts Guidelines also set out the scope of contractual clauses at Section 19.5 for recipients to comply with the required standard of protection in relation to personal data received so that it is comparable to the protection under the PDPA. The Key Concepts Guidelines sets out in a table (reproduced below) the areas of protection a transferring organisation should minimally set out in its contract in two situations: where the recipient is another organisation (except a data intermediary); and where the recipient is a data intermediary (i.e., an organisation that processes the personal data on behalf of the transferring organisation pursuant to a contract).

---

51 Regulation 9 of the PDP Regulations.
52 Regulation 10 of the PDP Regulations.
53 Regulation 9(3)(a) and 9(4)(a) of the PDP Regulations.
54 Regulation 9(2)(a) of the PDP Regulations.
55 Issued on 23 September 2013 and revised on 8 May 2015.
<table>
<thead>
<tr>
<th>S/N</th>
<th>Area of protection</th>
<th>Recipient</th>
<th>Data intermediary</th>
<th>Organisation (except data intermediary)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Purpose of collection, use and disclosure by recipient</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Accuracy</td>
<td></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Protection</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Retention limitation</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Policies on personal data protection</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Access</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Correction</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### V  PDPA AND COMPANY POLICIES AND PRACTICES

Organisations are obliged to develop and implement policies and practices necessary to meet their obligations under the PDPA. Organisations must also develop a complaints mechanism, and communicate to their staff the policies and practices they have implemented. Information on policies and practices, including the complaints mechanism, is to be made available on request. Every organisation is also obliged to appoint a data protection officer, who would be responsible for ensuring the organisation’s compliance with the PDPA, and to make the data protection officer’s business contact information publicly available.

As a matter of best practice, an organisation should have in place notices and policies that are clear, easily accessible and comprehensible. Some of the policies and processes that an organisation may consider having in place are set out below.

#### i  Data protection policy

If an organisation intends to collect personal data from individuals, it would be required to notify them of the purposes for the collection, use and disclosure of the personal data and seek consent before collecting the personal data. It should also state whether the personal data will be disclosed to third parties, and if so, who these organisations are. Further, where it is contemplated that the personal data may be transferred overseas, the organisation should disclose this and provide a summary of the extent to which the personal data would receive protection comparable to that under the PDPA, so that it may obtain consent from the individual for the transfer. The data protection policy may also specify how requests to access and correct the personal data may be made. To satisfy the requirement in the PDPA that data protection policies are available on request, the organisation may wish to make its policy available online.

---

56 Section 12(a) of the PDPA.
57 Section 12(b) of the PDPA.
58 Section 12(c) of the PDPA.
59 Section 12(d) of the PDPA.
60 Section 11(4) of the PDPA.
ii  **Cookie policy**
If the corporate website requires collection of personal data or uses cookies that require collection of personal data, users ought to be notified of the purpose for the collection, use or disclosure of the personal data, and prompted for their consent in that regard.

iii  **Complaints mechanism**
The organisation should develop a process to receive and respond to complaints it receives, and this should be made available to the public.

iv  **Contracts with data intermediaries**
Contracts with data intermediaries should set out clearly the intermediaries’ obligations, and include clauses relating to the retention period of the data and subsequent deletion or destruction, security arrangements, access and correction procedures, and audit rights of the organisation over the data intermediaries. Where a third party is engaged to collect data on an organisation’s behalf, the contract should specify that the collection is conducted in compliance with the data protection provisions.

v  **Employee data protection policy**
Employees should be notified of how their personal data may be collected, used or disclosed. The mode of notification is not prescribed, and the employer may choose to inform the employee of these purposes via employment contracts, handbooks or notices on the company intranet. Consent is not required if the purpose is to manage or terminate the employment relationship; as an example, the company should notify employees that it may monitor network activities, including company emails, in the event of an audit or review.

vi  **Retention and security of personal data**
Organisations should ensure that there are policies and processes in place to ensure that personal data are not kept longer than is necessary, and that there are adequate security measures in place to safeguard the personal data. An incident-response plan should also be created to ensure prompt responses to security breaches.

**VI PDPA AND DISCOVERY AND DISCLOSURE**
The data protection provisions under the PDPA do not affect any rights or obligations under other laws.61 As such, where the law mandates disclosure of information that may include personal data, another law would prevail to the extent that it is inconsistent with the PDPA. For instance, the Prevention of Corruption Act imposes a legal duty on a person to disclose any information requested by the authorities. Under those circumstances, the legal obligation to disclose information would prevail over the data protection provisions.

The PDPA has carved out specific exceptions in respect of investigations and proceedings. Thus, an organisation may collect data about an individual without his or her consent where the collection is necessary for any investigation or proceedings, so as not to compromise the availability or accuracy of the personal data.62 Further, an organisation may

---

61  Section 4(6) of the PDPA.
62  Second Schedule, Section 1(e) of the PDPA.
use personal data about an individual without the consent of the individual if the use is necessary for any investigation or proceedings.63 These exceptions, however, do not extend to internal audits or investigations. Nevertheless, it may be argued that consent from employees is not required as such audits would fall within the purpose of managing or terminating the employment relationship.64 Employees may be notified of such potential purposes of use of their personal data in their employee handbooks or contracts, as the case may be.

On an international scale, Singapore is active in providing legal assistance and in the sharing of information, particularly in respect of criminal matters. That said, the PDPC may not share any information with a foreign data protection body unless there is an undertaking in writing that it will comply with its terms in respect of the disclosed data. This obligation is mutual, and the PDPA also authorises the PDPC to enter into a similar undertaking required for a foreign data protection body where required.65

VII PDPA PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

The PDPC is the key agency responsible for administering and enforcing the PDPA. Its role includes, inter alia, reviewing complaints from individuals,66 carrying out investigations (whether on its own accord or upon a complaint), and prosecuting and adjudicating on certain matters arising out of the PDPA.67

To enable the PDPC to carry out its functions effectively, it has been entrusted with broad powers of investigation,68 including the power to require organisations to produce documents or information, and the power to enter premises with or without a warrant to carry out a search. In certain circumstances, the PDPC may obtain a search and seizure order from the state courts to search premises and take possession of any material that appears to be relevant to an investigation.

Where the PDPC is satisfied that there is non-compliance with the data protection provisions, it may issue directions to the infringing organisation to rectify the breach and impose financial penalties up to S$1 million.69 The PDPC may also in its discretion compound the offence.70 Certain breaches can attract penalties of up to three years’ imprisonment.71 In addition to corporate liability, the PDPA may also hold an officer of the company to be individually accountable if the offence was committed with his or her consent or connivance,

63 Third Schedule, Section 1(e) of the PDPA.
64 As discussed earlier, consent is not required if the purpose for the collection, use and disclosure of personal data is for managing or terminating the employment relationship.
65 Section 10(4) of the PDPA.
66 Section 28 of the PDPA.
67 See Sections 28(2) and 29(1) of the PDPA. The PDPC has the power to give directions in relation to review applications made by complainants and contraventions to Parts III to VI of the PDPA.
68 Section 50 of the PDPA. See also Ninth Schedule of the PDPA.
69 Section 29 of the PDPA.
70 Section 55 of the PDPA.
71 Section 56 of the PDPA.
or is attributable to his or her neglect.\textsuperscript{72} Further, employers are deemed to be vicariously liable for the acts of their employees, unless there is evidence showing that the employer had taken steps to prevent the employee from engaging in the infringing acts.\textsuperscript{73}

Directions issued by the PDPC may be appealed to be heard before the Appeal Committee. Thereafter, any appeals against decisions of the Appeal Committee shall lie to the High Court, but only on a point of law or the quantum of the financial penalty. There would be a further right of appeal from the High Court’s decisions to the Court of Appeal, as in the case of the exercise of its original civil jurisdiction.\textsuperscript{74}

In relation to breaches of the DNC Registry provisions, an organisation may be liable for fines of up to S$10,000 for each breach.

\textbf{ii} \hspace{0.5cm} \textbf{Recent enforcement cases}

In 2017, the PDPC published 19 decisions. In 2018, the number of published decisions stood at 17 by July 2018. In the decisions, the PDPC provides substantial factual detail and legal reasoning, and the decisions are another source of information for companies seeking guidance on particular issues.

Several enforcement actions in 2017 and the first half of 2018 set out the PDPC’s typical mix of behaviour remedies combined with financial penalties, including:

\textit{a} \hspace{0.5cm} \textit{Jiwon Hair Salon:}\textsuperscript{75} for the respondent’s failure to fulfil the openness obligation under Section 12(a) of the PDPA, the PDPC directed the respondent to put in place a data protection policy to comply with the provisions of the PDPA.

\textit{b} \hspace{0.5cm} \textit{Aviva Ltd (October 2017):}\textsuperscript{76} PDPC issued a fine of S$6,000 to multinational insurance company Aviva Ltd because the organisation failed to make reasonable security arrangements around the mailing of follow-up letters to its policyholders, which allowed the accidental mailing of documents meant for one policyholder to another policyholder.

\textit{c} \hspace{0.5cm} \textit{Aviva Ltd (April 2018):}\textsuperscript{77} in a matter similar to the October 2017 Aviva action, PDPC issued a fine of S$30,000 for failing to make reasonable security arrangements to prevent the unauthorised disclosure of personal data of policyholders, which allowed the accidental mailing of underwriting letters meant for three different clients to another client. In reaching its penalty, the Commissioner noted that this incident was ‘disappointingly similar’ to the October 2017 matter.

\textbf{iii} \hspace{0.5cm} \textbf{Private litigation}

Anyone who has suffered loss or damage directly arising from a contravention of the data protection provisions may obtain an injunction, declaration, damages or any other relief against the errant organisation in civil proceedings in court. However, if the PDPC has made a decision in respect of a contravention of the PDPA, no private action against the

\textsuperscript{72} Section 52 of the PDPA.
\textsuperscript{73} Section 53 of the PDPA.
\textsuperscript{74} Section 35 of the PDPA.
\textsuperscript{75} Decision Citation: [2018] SGPDPC 2.
\textsuperscript{76} Decision Citation: [2017] SGPDPC 14.
\textsuperscript{77} Decision Citation: [2018] SGPDPC 4.
organisation may be taken until after the right of appeal has been exhausted and the final decision is made.78 Once the final decision is made, a person who suffers loss or damage as a result of a contravention of the PDPA may commence civil proceedings directly.79

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS
The PDPA applies to foreign organisations in respect of activities relating to the collection, use and disclosure of personal data in Singapore regardless of their physical presence in Singapore.

Thus, where foreign organisations transfer personal data into Singapore, the data protection provisions would apply in respect of activities involving personal data in Singapore. These obligations imposed under the PDPA may be in addition to any applicable laws in respect of the data activities involving personal data transferred overseas.

IX CYBERSECURITY AND DATA BREACHES
i Data breaches
While the PDPA obliges organisations to protect personal data, it does not currently require organisations to notify authorities in the event of a data breach. However, as noted above, in the PDPC’s public consultation of July through September 2017, the PDPC proposed incorporating a mandatory reporting requirement in certain circumstances. In the absence of mandatory data breach requirements, government sector regulators have imposed certain industry-specific reporting obligations. For example, MAS issued a set of notices to financial institutions on 1 July 2014 to direct that all security breaches should be reported to MAS within one hour of discovery.

The Cybersecurity Act represents a move away from sector-based regulation. The Act requires mandatory reporting to the new Commissioner of Cybersecurity of ‘any cybersecurity incident’ (which is broader than but presumably would also include data breaches) that relates to CII or systems connected with CII. In issuing the bill, the government noted that it had considered sector-based cybersecurity legislation but had concluded that an omnibus law that would establish a common and consistent national framework was the better option.

ii Cybersecurity
Singapore is not a signatory to the Council of Europe’s Convention on Cybercrime.

In Singapore, the CMCA and the Cybersecurity Act are the key legislations governing cybercrime and cybersecurity. The CMCA is primarily focused on defining various cybercrime offences, including criminalising the unauthorised accessing80 or modification of computer material,81 use or interception of a computer service,82 obstruction of use of a computer,83

78 Section 32 of the PDPA.
80 Sections 3 and 4 of the CMCA.
81 Section 5 of the CMCA.
82 Section 6 of the CMCA.
83 Section 7 of the CMCA.
and unauthorised disclosure of access codes.84 The 2017 amendments to the CMCA added the offences of obtaining or making available personal information that the offender believes was obtained through a computer crime85 and using or supplying software or other items to commit or facilitate the commission of a computer crime.86

Although the CMCA is in general a criminal statute, the 2013 amendments added a cybersecurity provision in the event of certain critical cybersecurity threats. In particular, the Minister of Home Affairs may direct entities to take such pre-emptive measures as necessary to prevent, detect or counter any cybersecurity threat posed to national security, essential services or the defence of Singapore or foreign relations of Singapore.87

The Cybersecurity Act greatly expands national cybersecurity protections, including by imposing affirmative reporting, auditing and other obligations on CII owners and by appointing a new Commissioner of Cybersecurity with broad authority, including the power to establish mandatory codes of practice and standards of performance for CII owners.

X OUTLOOK

In keeping with its declared strategy, Singapore continues to progress on clarifying and enforcing its existing data privacy and cybersecurity regime.

84 Section 8 of the CMCA.
85 Section 8A of the CMCA.
86 Section 8B of the CMCA.
87 Section 15A of the CMCA. Essential services include the energy, finance and banking, ICT, security and emergency services, transportation, water, government and healthcare sectors.

© 2018 Law Business Research Ltd
I OVERVIEW

Data protection and privacy are distinct rights under Spanish law, but both are deemed fundamental rights derived from respect for the dignity of human beings. They are primarily based on the free choice of individuals to decide whether to share with others (public authorities included) information that relates to them (personal data) or that belongs to their private and family life, home and communications (privacy). Both fundamental rights are recognised in the Lisbon Treaty (the Charter of Fundamental Rights of the European Union) and the Spanish Constitution of 1978. Data protection rules address, inter alia, security principles and concrete measures that are helpful to address some cybersecurity issues, in particular, because specific cybersecurity legislation (which not only covers personal data and private information but rather any information) is new and not sufficiently developed yet.

Spain had an omnibus data protection framework law along the lines of the EU approach (mainly Law 15/1999 of 13 December on the Protection of Personal Data (the DP Law), as developed by Royal Decree 1720/2007 of 21 December (RD 1720/2007), jointly the DP Regulations), applying both to the private and public sectors. In addition, there are certain sector-specific regulations that also include data protection provisions.

The General Data Protection Regulation (GDPR) has not automatically repealed the DP Regulations; however, the DP Regulations remain in force only to the extent that they do not contravene the GDPR. For this reason, a new draft data protection law (the Draft Bill) is currently under discussion in the Spanish parliament that will provide for local rules and administrative proceedings adapted to the GDPR. Approval of the Draft Bill is expected by the end of 2018.

In addition, some personal data and or some processing activities may require specific protection such as certain financial, e-communications or health-related data or processing activities. There are several codes of conduct for data protection that were approved under former legal regime (i.e., the DP Regulations) in various sectors but, in general, they merely adjusted the general obligations to the specific needs of the corresponding sector or organisation. These codes will have to be reviewed pursuant to the GDPR.

The rights to data protection and privacy are not absolute and, where applicable, must be balanced with other fundamental rights or freedoms (e.g., freedom of information or expression) as well as other legitimate interests (e.g., intellectual property rights, public security and prosecution of crimes).

1 Leticia López-Lapuente and Reyes Bermejo Bosch are lawyers at Uría Menéndez Abogados, SLP.
In the case of data protection, this balance must be assessed by the organisation and could be challenged before the Spanish Data Protection Authority (DPA), which is in charge of supervising the application of the regulations on data protection (see Section III.i). Privacy infringements must be claimed before the (civil or criminal) courts.

The DPA was created in 1993, and has been particularly active in its role of educating organisations and the general public on the value of data protection and of imposing significant sanctions. In 2017 alone, the DPA received 10,651 claims from individuals and authorities, and issued and published 852 sanctioning resolutions within the private sector. These sanctions are published on the DPA’s website, which is used by the media (and others) as an important source of data protection information. However, as a consequence of the GDPR’s approval, the DPA is reviewing the contents to be published on its website (www.aepd.es) and it is likely that a significant part of the resolutions issued in the past will be removed from the website.

II THE YEAR IN REVIEW

In November 2017, the Draft Bill was published and submitted to the parliament for discussion and approval. This has been the most relevant milestone on data protection in Spain over the course of the past year. The initial wording of the Draft Bill has been subject to more than 300 proposed amendments by the different parliamentary groups and, thus, the draft is expected to change. Its approval is not expected until the end of 2018. Regarding the implementation of the Security of Network and Information Systems Directive (the NIS Directive), the Spanish government published a draft royal decree (see Section IX) that has not yet been sent to the parliament for discussion and approval.

Finally, as a consequence of the Google Spain v. Costeja (Google Spain) case in 2014 before the Court of Justice of the European Union (CJEU) (regarding the ‘right to be forgotten’), the DPA has continued to initiate certain proceedings on this matter; several judicial rulings of relevance on a national level (mainly from the Spanish Supreme Court) have been issued in Spain modulating the scope of the ‘right to be forgotten’. In this regard, more recently, on 4 June 2018, the Spanish Constitutional Court has issued its first ruling regarding the scope and nature of the ‘right to be forgotten’ (see Section VII.ii). The relevance of this ruling is that the Spanish Constitutional Court has recognised that the ‘right to be forgotten’ has an independent nature from the data protection rights.

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

The legal framework for the protection of personal data in Spain is regulated by the Lisbon Treaty; Article 18(4) of the Spanish Constitution; the GDPR and, until approval of the Draft Bill, by those provisions of the DP Regulations that are compatible with the GDPR.

Sector-specific regulations may also contain data protection provisions, such as the E-Commerce Law 34/2002 (LSSI), the General Telecommunications Law 9/2014 (GTL), anti-money laundering legislation or the regulations on biomedical research. However, they generally refer to the DP Regulations and, now that the GDPR is in force, will either be subject to review or should at least be reinterpreted according to GDPR rules.
Privacy rights are mainly regulated by the Spanish Constitution, Law 1/1982 of 5 May on civil protection of the rights to honour, personal and family privacy, and an individual’s own image, and by the Spanish Criminal Code.

Personal data and private data are not synonymous. Personal data are any kind of information (alphanumeric, graphic, photographic, acoustic, etc.) concerning an identified or identifiable natural person, irrespective of whether or not this information is private. However, data regarding ideology, trade union membership, religion, beliefs, racial origin, health or sex life as well as criminal and administrative offences are deemed more sensitive and require specific protection.

Protecting personal data is achieved by allocating specific duties to both ‘controllers’ (i.e., those who decide on the data processing purposes and means) and ‘processors’ (i.e., those who process the data only on behalf of a controller to render a service).

The DPA is the entity in charge of supervising compliance with the data protection duties imposed by the GDPR and DP Regulations (fair information, legitimate ground, security, notification, proportionality and quality, etc.). The DPA has carried out ex officio audits of specific sectors (including online recruitment procedures, TV games and contests, hotels, department stores, distance banking, hospitals, schools, webcams and mobile apps). However, the DPA’s activity in terms of individual compliance investigations has significantly increased over the past 10 years, as has the number of fines imposed. Indeed, failure to comply with the GDPR and DP Regulations may result in the imposition of administrative fines depending on the severity of the offence (and regardless of whether civil or criminal offences are also committed, if applicable). Neither harm nor injury is required (i.e., the infringement itself suffices for the offender to be deemed liable), but the lack of any harm or injury is considered an attenuating circumstance to grade the amount of the administrative fine. However, harm or injury will be required to claim damages arising from breaches of data protection rights before civil and criminal courts.

**ii General obligations for data handlers**

Since the Draft Bill has not been approved, the main obligations of data controllers and data processors are those set out in the GDPR.

**Obligations of data controllers**

- Any processing activity should be internally monitored and, in certain cases, duly registered and documented;
- data subjects from whom personal data are requested must be provided beforehand with information about the processing of their personal data (the DPA has published specific guidelines to comply with the GDPR rules on information duties);
- the processing of personal data must be based on a legitimate ground, among others, have the prior and explicit consent of the data subject, be based on the existence of a contractual relationship that makes the processing unavoidable, the existence of a legal obligation imposed on the controller or a legitimate interest;

---

2 The data protection right is enforced by the DPA at a national level with limited exceptions. For example, Catalonia and the Basque country are regions that have regional data protection authorities with competence limited to the processing of personal data by the regional public sector.
when the recipient is not located in the EU or EEA (or in a country whose regulations afford an equivalent or adequate level of protection identified by the European Commission or the DPA), appropriate guarantees must be adopted, unless a legal exemption applies;

c) controllers should adopt appropriate security measures, as explained in Section IX; and

d) data subjects have a right to access all data relating to them, to rectify their data and have their data erased if the processing does not comply with the data protection principles, in particular, when data are incomplete, inaccurate or excessive in relation to the legitimate purpose of its processing. Data subjects are also entitled to object to certain processing activities that do not require their consent or are made for direct marketing purposes, as well as to request the restriction of processing and the portability of their data.

Obligations of data processors

Data processors must:

a) execute a processing agreement with the relevant data controller;

b) implement the above-mentioned security measures;

c) process data only to provide the agreed services to the controller and in accordance with its instructions;

d) keep the data confidential and not disclose it to third parties (subcontracting is not prohibited but is subject to specific restrictions); and

e) upon termination of the services, return or destroy the data, at the controller's discretion.

In addition to the above, the GDPR has added specific mandatory content for a processing agreement to be valid (as provided by Article 28.3 of the GDPR) including the duty to provide assistance to the controller in the event of data breaches or the duty to allow audits to its processing of data. Since the duties under the GDPR became applicable as from May 2018, the DPA has published specific guidelines on how to comply with the GDPR rules regarding processing agreements.

iii Specific regulatory areas

The DP Regulations apply to any personal data, but they provide for reinforced protection of data related to children (e.g., the verifiable consent of the minor's parents is required) and to certain categories of especially protected data, such as health-related data (e.g., they may require the performance of a privacy impact assessment). Under local laws (i.e., the DP Regulations) specific rules also apply to the information processed by solvency and credit files, and to the processing of data for video surveillance or access control purposes. Some of these matters are proposed to be specifically regulated also in the Draft Bill and, thus, the final version of the Draft Bill will be highly relevant for these processing activities.

In addition, certain information is also protected by sector-specific regulations. This is the case for, inter alia:

a) financial information that is subject to banking secrecy rules (Law 10/2014 of 26 June 2014 on the regulation, supervision and solvency of credit institutions);

b) the use (for purposes other than billing) and retention of traffic and location data (GTL);
the sources of information and intra-group disclosures to comply with regulations concerning anti-money laundering and combating the financing of terrorism, and restrictions on the transparency principle in relation to data subjects (Law 10/2010 of 28 April on the prevention of money laundering and financing of terrorism);

the use of genetic data or information contained in biological samples (Law 14/2007 of 3 July on biomedical research);

information used for direct-marketing purposes (LSSI);

the outsourcing of core financial services to third parties (Royal Decree 84/2015 of 13 February developing Law 10/2014, and Bank of Spain Circular 2/2016 on the supervision and solvency of credit institutions, which adapts the Spanish legal regime to EU Directive 2013/36/EU and EU Regulation 575/2012); and

the use of video-surveillance cameras in public places (Law 4/1997 of 4 August governing the use of video recording in public places by state security forces).

Since the above regulations generally refer to the DP Regulations and after May 2018 they will need to be reviewed according to the GDPR or, at least, reinterpreted according to GDPR rules.

iv Technological innovation

Technology has created specific issues in the privacy field, including:

a online tracking and behavioural advertising: as a general rule, explicit prior consent is required. The DPA does not generally consider that online behavioural advertising or profiling activities can be based on the existence of a legitimate interest. In addition, the DPA has expressly announced that profiling activities must be considered as separate processing activities from any others, such as advertising ones, and, as such, a specific and separate legal ground must legitimate these activities (e.g., a separate consent);

b location tracking: the DPA considers that the use of this technology in work environments may be reasonable and proportionate and subject to certain requirements (mainly, that specific information has been previously provided to data subjects on the potential monitoring of IT resources);

c use of cookies: as a general rule, explicit prior consent is required for installing cookies or similar devices on terminal equipment. In June 2018 the DPA announced that cookie policies must be adjusted according to the GDPR’s requirements and has issued certain guidelines on how banners and privacy policies should be adapted accordingly. In 2017, the DPA initiated 395 investigations and issued 55 sanctioning resolutions regarding Internet services (certain of which included the use of cookies);

d biometrics: traditionally, the processing of biometric data has not been considered ‘sensitive’ and, therefore, the DPA has made no specific requirements in this area. The implementation of the GDPR in Spain implies a change in the concept of biometrics, which are now considered especially protected data, and we are currently awaiting the DPA’s guidelines in this regard;

e big data analytics: in April 2017, the DPA published guidelines on how to implement big data projects according to GDPR rules;

f anonymisation, de-identification and pseudonymisation: the DPA has adopted an official position regarding the use of ‘anonymous’ data and open data in big data projects.
In particular, the DPA published guidelines at the end of 2016 on the protection of personal data related to the reuse of public-sector information and guidelines on anonymisation techniques;

g internet of things and artificial intelligence: the DPA has not adopted an official position regarding the internet of things and artificial intelligence;

h data portability: the DPA has published a legal report on, among other issues, the data portability right. The DPA stated that the portability right includes not only data subjects' current data, but also their former data (either provided by them or inferred from the contractual relationship); however, the information obtained from the application of profiling techniques (e.g., algorithms) would not be subject to portability. Although the DPA’s legal reports are not binding, they are highly useful since they reflect the DPA's doctrinal tendency;

i right of erasure or right to be forgotten: the right to be forgotten in relation to search engines is actively pursued both by Spanish data subjects and the DPA. Notably, Google Spain, in which the CJEU’s ruling recognised the right to be forgotten, was initiated in Spain and the Spanish DPA had a significant role in the case. There are several DPA resolutions issued every year recognising the right of Spanish individuals to be forgotten and also setting out certain exceptions to the applicability of the right. Recently, the Spanish Constitutional Court, in its ruling dated 4 June 2018, confirmed this approach and has recognised the right to be forgotten as a new fundamental right, different but related to data protection rights; and

j data-ownership issues: to date, there is no Spanish legislation that specifically regulates the question of ownership of data. Notwithstanding this, several regulations exist that may have an impact on data ownership including, among others, data protection legislation, copyright law (which regulates rights over databases) or even unfair competition rules.

IV INTERNATIONAL DATA TRANSFER AND DATA LOCALISATION

According to the DP Regulations, data transfers from Spain to (or access by) recipients located outside the EEA used to require the prior authorisation of the DPA, unless the transfer could be based on a statutory exemption. Even though these rules, contained in the DP Regulations, have not been formally repealed when the GDPR became applicable in May 2018, these local rules are considered to be incompatible with the GDPR’s regime on international transfers of data and, thus, are considered inapplicable. For this reason, GDPR’s regime on international transfers is the only regime that applies to transfers in Spain. Also, the Draft Bill that will contain the new data protection law is not expected to include changes to the GDPR’s general regime.

Turning to data localisation, there are no specific restrictions in Spain; however, along with the GDPR (which imposes certain restrictions and requirements on disclosing data to non-EU entities), there are specific laws imposing requirements that could be understood as 'restrictive measures', including, among others, tax regulations (Royal Decree 1619/2012 of 30 November on invoicing obligations), gambling regulations (Royal Decree 1613/2011)
and specific public administration regulations (Law 9/1968 of 5 April on secrecy pertaining to official issues, Law 38/2003 of 17 November on subsidies and Law 19/2013 of 9 December on transparency and access to public information).

V COMPANY POLICIES AND PRACTICES

i Privacy and security policies
Organisations that process personal data must comply with the accountability principle and, thus, are required to have both ‘general’ and ‘specific’ privacy policies, protocols and procedures. In addition, such policies are useful for (1) complying with the information duties regarding processing activities (see Section III.ii) and (2) complying with the duty to have all employees aware of the applicable security rules since organisations must implement appropriate technical and organisational measures to ensure a level of security that is commensurate with the risk (see Section IX).

Privacy officers
Before May 2018, a chief privacy officer was not mandatory, but in practice this role was deemed crucial for the controller or the processor to comply with the DP Regulations, in particular when the organisation is complex or if the data processed are sensitive or private.

From May 2018, several Spanish data controllers and processors are required to appoint a data protection officer according to Article 37 of the GDPR. Although the Draft Bill of the new data protection law is not definitive, it is expected to expand and detail more the cases in which the appointment of a data protection officer will be mandatory.

Under DP Regulations, the appointment of a security officer was required under certain circumstances but from 25 May 2018, the appointment of this role is no longer mandatory.

Privacy impact assessments
Privacy impact assessments have been mandatory for certain data processing as from May 2018. For this reason, the DPA recently published guidelines on privacy impact assessments. However, the DPA has been encouraging the adoption of privacy impact assessments in certain cases (e.g., big data projects) since 2014 (when it published its first guidelines on the matter). Finally, it must be noted that the Draft Bill also includes a list of cases in which a privacy impact assessment must be carried out (e.g., when the processing involves data subjects in special conditions of vulnerability or when special categories of data are processed and the processing is not merely incidental or accessory).

Work councils
Any employee representative in the organisation is entitled to issue a non-binding report before the implementation of new methods of control of the work. Although it is unclear what qualifies as a ‘method of control’ of the work, it is advisable to inform the works council of the implementation of new methods (e.g., whistle-blowing systems) and offer their members the possibility of issuing the above-mentioned non-binding report before its implementation.
VI DISCOVERY AND DISCLOSURE

Non-EU laws are not considered, as such, a legal basis for data processing, in particular regarding transfers to foreign authorities and especially if they are public authorities. This approach is consistent with Article 6.3 of the GDPR.

E-discovery and any enforcement requests based on these laws require a complex case-by-case analysis from a data protection, labour and criminal law point of view (and other sector-specific regulations, such as bank secrecy rules).

From a data protection point of view, the Spanish DPA’s position is the one adopted by all EU DPAs in the Guidelines on Article 49 of Regulation 2016/679 adopted by the Article 29 Working Party. According to this joint position, data transfers for the purpose of formal pretrial discovery procedures in civil litigation or administrative procedures may fall under derogation of Article 49 of the GDPR. According to the DPAs, this rule of the GDPR can also cover actions by the data controller to institute procedures in a third country, such as commencing litigation or seeking approval for a merger. Notwithstanding this, the derogation cannot be used to justify the transfer of personal data on the grounds of the mere possibility that legal proceedings or formal procedures may be brought in the future.

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

The DPA is the independent authority responsible for the enforcement of the GDPR and DP Regulations and the data protection provisions of the LSSI and the GTL.

Among other powers and duties, the DPA has powers that include the issuing of (non-binding) legal reports, recommendations, instructions and contributions to draft rules; powers of investigation; and powers of intervention, such as ordering the blocking, erasing or destruction of unlawful personal data, imposing a temporary or definitive ban on processing, warning or admonishing the controller or processor, or imposing administrative fines (fines are only imposed on private-sector entities). The DP Regulations establish three classifications of infringements (and their correlative administrative fines): minor, serious and very serious, resulting in administrative fines ranging from €900 to €600,000 depending on the severity of the infringement. However, this former sanctioning regime, although not officially repealed, was considered incompatible with GDPR rules and, thus, inapplicable from 25 May 2018. Thus, the applicable sanctioning regime under the GDPR did not have a full set of compatible local administrative rules to operate and implement the sanctions. Since this could have caused some formal problems, the Spanish government approved in July 2018 an urgent partial legal reform of sanctioning regime that allows sanctions under the GDPR to fully operate in Spain at least until the Draft Bill is finally passed.

Disciplinary procedures start ex officio, but generally stem from a complaint submitted by any person (e.g., the data subject, consumer associations, competitors or former employees).

The DPA is very active: in addition to ex officio inspections of specific sectors (always announced in advance), in 2017 (the most recent official statistics published by the DPA): 11,617 complaints from individuals were solved; over 1,200 sanctioning resolutions were
issued; and the fines imposed amounted to approximately €17.3 million. Most of the sanctions imposed on the private sector were for lack of consent and breach of the quality principle.

ii Recent enforcement cases

The following are the most significant enforcement issues to have arisen in Spain in the period 2017–2018.

The DPA has carried out numerous disciplinary proceedings related to the disclosure of data to solvency and credit agencies (284), to unlawful contracting (131) and unsolicited marketing (124). The DPA has also issued several reports assessing the application of the legitimate interest as a legitimate ground for the processing, including a legal report issued as a response to the Spanish Banking Association’s questions on this matter or the Guidelines on how to carry out big data projects.

In addition, the number of proceedings carried out and sanctions imposed by the DPA against non-Spanish and non-EU controllers has also increased. In fact, the DPA is participating in coordinated activities with other EU authorities to investigate companies that are based in the United States but carry out intensive processing activities in the EU.

Finally, the Spanish Constitutional Court has issued a significant ruling (ruling dated 4 June 2018) assessing the scope of the right to be forgotten in a wide manner. In particular, the Spanish Constitutional Court has set out the right to be forgotten may include not only the duty of the internet search engine to remove the relevant links, but also an additional duty of the relevant media or newspaper that initially published the information to remove the personal information from the news in its internal site’s search engines. Moreover, this ruling considers the right to be forgotten as a new and separate constitutional right.

iii Private litigation

Data subjects may claim damages arising from the breach of their data protection rights before the civil courts. Claims for civil damages usually involve pecuniary or moral damages, or both, linked to the violation of honour (such as the improper disclosure of private information) and privacy rights (such as the dissemination of private images). In general, indemnities granted to date have been exceptional and have not exceeded €3,000 (with limited exceptions such as one awarding €20,000). Notwithstanding this, recognition under the GDPR of the possibility to initiate class actions related to data protection matters has created a new framework and there are news in the market around the potential initiation by Spanish consumers association of class actions related to data protection alleged infringements.

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

The application of the DP Regulations for foreign organisations was triggered by either the existence of a data processor or processing equipment in Spain or, according to Google Spain, the existence of an establishment in Spain the activity of which is inextricably linked to that of the foreign organisation. Following 25 May 2018, after GDPR rules became applicable, the extraterritorial applicability of EU data protection legal framework is reinforced as a result of the GDPR’s territorial scope rules under Article 3.2 of the GDPR.

According to them, offering goods and services to EU citizens and online tracking addressed to the EU or Spanish market may trigger the application of the data protection
provisions not only of the GDPR but also of the LSSI, as well as the consumer regulations (only if consumers resident in Spain are involved), irrespective of where the organisation is established.

IX CYBERSECURITY AND DATA BREACHES

The approval in July 2016 of the NIS Directive was the most significant cybersecurity milestone in recent years. It marks the first instance of EU-wide rules on cybersecurity. The NIS Directive has not yet been implemented into Spanish law, although the government has published a first draft of a law that is consistent with the EU approach. Until implementation occurs, the regulation of cybersecurity matters in Spain will remain diffuse and insufficient, particularly in light of the steady rise in cybersecurity attacks involving Spanish organisations and infrastructure. Furthermore, as a consequence of cybersecurity, the number of cybersecurity certifications has also increased. However, a clear market leader has yet to emerge.

The DPA has also been highly active in relation to cybersecurity matters. Following certain global attacks, the DPA published a post in its website regarding ransomware attacks and how to guard against them. Among other recommendations, the DPA made the following key points: (1) companies should have a complex security plan for the protection of their networks (including a training plan for staff and the continuous updating of all software programs used by the company – especially those used for antivirus purposes); (2) they should have an action plan for how to react in the event of an attack; and (3) they should have a remedial plan to be implemented once the attack is contained.

Also, during 2017 and 2018 the DPA has published other guidelines regarding how to react in the event data breaches including general ‘Guidelines on how to manage and notify data breaches’ and the ‘Guidelines on how to manage an information leakage in law firms’.

As to criminal law, the Spanish Criminal Code was amended in 2010 to implement the Convention on Cybercrime and Council Framework Decision 2005/222/JHA on attacks against information systems. Specifically, this entailed the introduction of two new criminal offences:

\[a\] the discovery and disclosure of secrets – namely, the unauthorised access to data or applications contained in an IT system – by any means and infringing implemented security measures; and

\[b\] the intentional deletion, damage, deterioration, alteration or suppression of data, applications and electronic documents of third parties rendering them unavailable, as well as the intentional serious hindering or interruption of the functioning of an information system.

Other criminal offences that could be related to cybercrime were also modified (computer fraud, sexual offences, technological theft, and offences against intellectual and industrial property). The Criminal Code was amended again in March 2015. Specifically, aligned with European regulations on computer-related offences, the following new criminal offences are regulated: (1) intercepting data from information systems for the discovery and disclosure of secrets; and (2) creating computer programs or equipment for the purposes of discovering and disclosing secrets or committing damage to IT systems. Finally, legal entities can be held criminally liable for the above-mentioned offences.
Without prejudice to the above, there are no cybersecurity laws and requirements applicable to organisations ‘generally’, but rather a certain number of rules that address specific cybersecurity issues:

In 2012, the security breach notification regime was introduced in Spain through the GTL in line with Directive 2009/136/EC: the providers of public communications networks or publicly available electronic communications services must notify any security breaches, when personal data are involved, to both the data subjects and the DPA. In March 2014, the DPA approved an online system to notify security breaches. The requirements of the notification itself are those established in EU Regulation 611/2013. Since the notification of data breaches is not mandatory in general (except for the above-mentioned service providers), most of them remain unknown to the DPA and the public. One of those made public was the security breach suffered by BuyVip (which belongs to the Amazon group) in 2011, which involved the names, dates of birth, email addresses, phone numbers and shipping addresses of its customers. Although BuyVip was not subject to a notification duty in Spain, it decided to inform all its users of the security breach, and the notice went viral on the internet. The DPA then initiated an *ex officio* investigation, but the sanction imposed on BuyVip, if any, was not made public.

The LISS was amended in 2014 to establish specific obligations on cybersecurity incidents applicable to information society services providers, domain name registries and registrars. These obligations are twofold:

a. to collaborate with the relevant computer emergency response teams to respond to cybersecurity incidents affecting the internet network (to this end, the relevant information – including IP addresses – must be disclosed to them, but ‘respecting the secrecy of communications’); and

b. to follow specific recommendations on the management of cybersecurity incidents, which will be developed through codes of conduct (these have not yet been developed).

Operators of critical infrastructure⁶ (entities responsible for investments in, or day-to-day operation of, a particular installation, network, system, physical or IT equipment designated as such by the National Centre for Critical Infrastructure Protection (CNPIC) under Law 8/2011) are subject to specific obligations, such as providing technological assistance to the Ministry of Home Affairs, facilitating inspections performed by the competent authorities, and creating the specific protection plan and the operator’s security plan.

Furthermore, these operators must appoint a security liaison officer and a security officer. The security liaison officer requires a legal authorisation (issued by the Ministry of Home Affairs), and his or her appointment must be communicated to this Ministry. The security officer does not need a legal authorisation, but his or her appointment must nevertheless be communicated to the relevant government delegation or the competent regional authority.

Royal Decree 3/2010 establishes the security measures to be implemented by Spanish public authorities to ensure the security of the systems, data, communications and e-services addressed to the public, and they could apply by analogy. These security measures are classified into three groups: the organisational framework, which is composed of the set of measures relating to the overall organisation of security; the operational framework, consisting of

---

⁶ The following infrastructure areas have been considered ‘critical’ by Law 8/2011 (which transposes Directive 2008/114/EC into Spanish law): administration, water, food, energy, space, the chemical industry, the nuclear industry, research facilities, health, the financial and tax system, ICT and transport.
the measures to be taken to protect the operation of the system as a comprehensive set of components organised for one purpose; and protection measures, focused on the protection of specific assets according to their nature, and the required quality according to the level of security of the affected areas. Spanish law does not directly address restrictions to cybersecurity measures.

Although cybersecurity requirements do not specifically refer to personal data (but rather to any kind of information), specific security measures will have to be implemented when personal data are involved. In particular, the GDPR requires controllers and processors to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. There is no a mandatory list of security measures to be implemented; however, RD 1720/2007 provides a list of security measures (e.g., establishing an incidents record), distinguishing three levels of security measures depending on the nature of the data, which can be used as a standard specially for SMEs (taking into account the state of the art; costs of implementation; and nature, scope, context and purposes of processing as well as the risk of the varying likelihood and severity for the rights and freedoms of natural persons).

In addition to the above-mentioned laws, certain authorities with specific cybersecurity responsibilities have issued guidance, such as:

- the guidelines published by the Spanish National Institute of Cybersecurity (INCIBE) in 2015 regarding, inter alia:
  - how companies should manage information leaks;
  - cybersecurity on e-commerce;
  - security-related risk management for companies; and
  - protocols and network security in industrial control systems infrastructures;
- the publication by INCIBE in 2016 of a consolidated code of cybersecurity rules in Spain;
- the National Cybersecurity Strategy issued by the presidency in 2013;
- the strategy series on cybersecurity issued by the Ministry of Defence; and
- the Supervisory Control and Data Acquisition Guidelines issued by the CNPIC in collaboration with the National Cryptological Centre (CNN) in 2010.

The agencies and bodies with competences on cybersecurity are numerous:

- the CCN, which is part of the National Intelligence Centre;
- the CCN Computer Emergency Response Team;
- the CNPIC;
- the Cybersecurity Coordinator’s Office (which is part of the CNPIC);
- the Secretary of State for Telecommunications and Information Society; and
- INCIBE (previously known as the National Institute of Communication Technologies), which is the public sector company in charge of developing cybersecurity.

### X OUTLOOK

Data protection is constantly evolving. In the past, it has been neglected by both private and public organisations or deemed an unreasonable barrier for the development of the economy. However, this trend has definitively changed in the past five years.

This change is mostly due to the sanctions imposed by the DPA, the role of data in the development of the digital economy (the ‘data driven economy’), the active voice of users in the digital environment (developing new social interactions and not only acting as
consumers) and the fact that the European Commission and the European Parliament have definitively embraced a strong ‘privacy mission’. Decisions of the CJEU (such as in the Schrems v. Facebook or in the Google v. Costeja cases) have also sent out a clear message on the importance of data protection rules in Europe.

The adoption in 2016 of the GDPR constituted a significant milestone in the construction of a new data protection environment. In Spain, the Spanish parliament is currently working on the approval of the Draft Bill, although this approval is not expected before the end of 2018. Although the GDPR provides for data protection principles that are similar to those of the former DP Regulations, as construed by the CJEU and the Article 29 Working Party, it also provides for new rules and standards. Spanish organisations are particularly concerned about the new fines (the applicable criteria for which would be similar to those used in antitrust regulations – a percentage of annual worldwide turnover), the accountability principle, the general security breach notification and the mandatory implementation of a data-protection officer. Additional requirements regarding information and consent duties set out in the GDPR will also be a challenge for Spanish data controllers.

Also, changes in the regulation of the cybersecurity legal regime are expected to happen in Spain in the next year, particularly if the NIS Directive is finally implemented.
Chapter 23

SWITZERLAND

Jürg Schneider, Monique Sturny and Hugh Reeves

I OVERVIEW

Data protection and data privacy are fundamental constitutional rights protected by the Swiss Constitution. Swiss data protection law is set out in the Swiss Federal Data Protection Act of 19 June 1992 (DPA) and the accompanying Swiss Federal Ordinance to the Federal Act on Data Protection of 14 June 1993 (DPO). Further data protection provisions governing particular issues (e.g., the processing of employee or medical data) are spread throughout a large number of legislative acts. As Switzerland is neither a member of the European Union (EU) nor of the European Economic Area (EEA), it has no general duty to implement or comply with EU laws. Accordingly, Swiss data protection law has some peculiarities that differ from the legal framework provided by the EU General Data Protection Regulation (GDPR). However, because of Switzerland’s location in the centre of Europe and its close economic relations with the EU, Swiss law is in general strongly influenced by EU law, both in terms of content and interpretation. A closer alignment of Swiss data protection law with the GDPR is also one of the aims of the ongoing reform of the DPA, which the Swiss Federal Council initiated in April 2015.

The Swiss Data Protection and Information Commissioner (Commissioner) is the responsible authority for supervising both private businesses and federal public bodies with respect to data protection matters. The Commissioner has published several explanatory guidelines that increase legal certainty with respect to specific issues such as data transfers abroad, technical and organisational measures, processing of data in the medical sector and processing of employee data. Despite the lack of drastic sanctions in respect of data protection under the current legislative regime, it is nonetheless a topic at the forefront of public attention in Switzerland, especially given the active presence of the Commissioner and the high level of media attention given to data protection matters.

1 Jürg Schneider is a partner, Monique Sturny is a managing associate and Hugh Reeves is an associate at Walder Wyss Ltd.
2 Classified compilation (SR) 235.1, last amended as of 1 January 2014.
3 Classified compilation (SR) 235.11, last amended as of 16 October 2012.
4 Specific duties exist in certain areas based on international treaties. Furthermore, the GDPR, which became effective on 25 May 2018, is not only relevant for companies located in EU and EEA Member States, but also for Swiss companies under certain circumstances, see Section II below for more detail.
5 Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
6 The guidelines are not legally binding, but do set de facto standards.
II THE YEAR IN REVIEW

Of a number of noteworthy reforms initiated back in 2015, some are still pending and some are expected to enter into force shortly or entered into force recently.

On 1 April 2015, the Swiss Federal Council formally decided to undertake a revision of the DPA, which is still ongoing. The overarching aim of the ongoing reform of the DPA is – among others – to lay the foundations for Switzerland’s ratification of the modernised Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) and, where necessary in the context of the further development of the Schengen/Dublin acquis, the adaptation of the DPA to the GDPR (see Section X, for more details).

On 21 December 2016, the Federal Council issued a preliminary draft of the revised DPA. This preliminary draft was subject to a public consultation process, which ended on 4 April 2017 and, in late August 2017, the Federal Council released the results and the various opinions gathered throughout the consultation process. This in turn resulted in the establishment of a revised draft accompanied by an explanatory report of the Swiss Federal Council on 15 September 2017. Subsequently to the publication of the revised draft DPA, the Swiss federal parliament decided that the revision shall be split in two phases.

In a first step, the necessary amendments shall be adopted in order to implement the Schengen/Dublin framework (EU Directive dated 27 April 2016, EC 2016/680) regarding data protection in the field of criminal prosecution as well as police and judicial cooperation.

In a second step, the remaining main revision of the DPA, which will align Swiss data protection law more closely to the substantive provisions of the GDPR and ensure compliance with the revised Council of Europe Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data (revision of ETS No. 108, 28 January 1981) shall be discussed by the parliament. The final text will be subject to an optional referendum.

Owing to the splitting of the revision into two phases, the data protection reform will be somewhat delayed compared to the initial schedule. Entry into force of the revised DPA is now tentatively scheduled for 2019 for the first step relating to compliance with the EU Schengen/Dublin acquis and 2020 for the remaining main revision of Swiss data protection law.

The revision process of the Swiss Federal Act on the Supervision of Postal and Telecommunication Services of 18 March 2016 was successfully terminated, and the revised

7 The draft DPA, the explanatory report of the Swiss Federal Council and the summary of the results of the consultation process are available in German, French and Italian on the website of the Swiss Confederation at: (in German) www.ejpd.admin.ch/ejpd/de/home/aktuell/news/2017/2017-09-150.html; (in French) www.ejpd.admin.ch/ejpd/fr/home/aktuell/news/2017/2017-09-150.html; and (in Italian) www.ejpd.admin.ch/ejpd/it/home/aktuell/news/2017/2017-09-150.html (all sites last visited on 21 July 2018). An unofficial English translation of the draft DPA can be found at: https://www.dataprotection.ch/dpa-revision/documentation-and-english-translation/.

8 Classified compilation (SR) 780.1.
Act and the revised related ordinance\(^9\) entered into force on 1 March 2018.\(^{10}\) The main changes concern in particular the monitoring of new technologies, the tasks of the competent authority, the personal scope of application and the storage of data.\(^{11}\)

The new Swiss Federal Act on Intelligence Service (the Intelligence Service Act) was approved in a referendum in September 2016 and entered into force, together with its related ordinance, on 1 September 2017.\(^{12}\) The new Intelligence Service Act will bring increased monitoring competence for Swiss intelligence services and was predominantly driven by increased efforts to prevent terrorism. The expansion of surveillance options has been heavily debated and criticised for undermining privacy and other fundamental rights of data subjects.

Many Swiss companies have been conducting GDPR implementation projects recently due to the wide extraterritorial scope of application of the GDPR, and also in anticipation of the expected changes to Swiss data protection law that will bring a closer alignment of the Swiss provisions to the GDPR. The GDPR applies to the processing activities of many Swiss companies as it applies, \textit{inter alia}, to data processing activities outside the EU and EEA that have effects in the EU or EEA (the effects doctrine). In particular, the GDPR applies to Swiss companies in connection with the targeted offering of goods or services to persons in the EU and EEA or the monitoring of behaviour of persons in the EU and EEA (Article 3 GDPR). In addition, the GDPR may become applicable if a person with habitual residence in the EU or EEA were to claim the applicability of the law of his or her state of habitual residence based on Article 139 Paragraph 1 Letter (a) of the Swiss Federal Act on Private International Law of 18 December 1987\(^{13}\) (PILA) or, if the effects of an infringement of personality rights through the processing of personal data occurred in the EU or EEA, the injured person may claim the applicability of the law of the state in which the effects of the damaging act occurred and the infringing party should have foreseen that the effects would occur in that state (Article 139 Paragraph 1 Letter (b) and Paragraph 3 PILA).

\section*{III \textbf{REGULATORY FRAMEWORK}}

\textbf{i Privacy and data protection legislation and standards}

\textit{Privacy and data protection laws and regulations}

The Swiss Constitution of 18 April 1999\(^{14}\) guarantees the right to privacy in Article 13. The federal legislative framework for the protection of personal data mainly consists of the DPA and the DPO. Further relevant data protection provisions are contained in the Federal Ordinance on Data Protection Certification of 28 September 2007.\(^{15}\) Specific data protection issues such as, \textit{inter alia}, transfers of data abroad, and data protection in relation to employees or as regards the medical sector, are dealt with in more detail in the relevant guidelines published by the Commissioner.\(^{16}\)

\begin{itemize}
  \item[9] Ordinance on the Supervision of Postal and Telecommunication Services of 18 March 2016, classified compilation (SR) 780.11.
  \item[10] Classified compilation (SR) 780.1 and SR 780.11.
  \item[12] Classified compilation (SR) 121 and SR 121.1.
  \item[14] Classified compilation (SR) 101, last amended as of 12 February 2017.
  \item[15] Classified compilation (SR) 235.13, last amended as of 1 November 2016.
  \item[16] As mentioned in footnote 8, the guidelines are not legally binding, but do set \textit{de facto} standards.
\end{itemize}
The DPA and DPO apply to data processing activities by private persons (i.e., individuals and legal entities) and by federal bodies. In contrast, data processing activities by cantonal and communal bodies are regulated by the cantonal data protection laws and supervised by cantonal data protection commissioners, who also issue guidance within their scope of competence. Hence, data processing activities of cantonal and communal bodies are subject to slightly different regimes in each of the 26 cantons. Unless explicitly set forth otherwise, the present chapter focuses on the Swiss federal legislation without addressing the particularities of the data protection legislation at the cantonal level.

**Key definitions under the DPA**

- **a** Personal data (or data): all information relating to an identified or identifiable person. Unlike the data protection laws of most other countries, Swiss data protection law currently protects personal data relating to both individuals and legal entities. Hence, the term ‘person’ refers not only to natural persons (individuals), but also to legal entities such as corporations, associations, cooperatives or any other legal entity, as well as partnerships. It is expected, however, that personal data relating to legal entities will no longer be protected under the revised DPA.

- **b** Data subject: an individual or, currently, also a legal entity whose data is being processed.

- **c** Processing of personal data: any operation with personal data, irrespective of the means applied and the procedure, and in particular the storage, use, revision, disclosure, archiving or destruction of data.

- **d** Sensitive personal data: data relating to:
  - religious, ideological, political or trade union-related views or activities;
  - health, the intimate sphere or racial origin;
  - social security measures; and
  - administrative or criminal proceedings and sanctions.

- **e** Personality profile: a collection of data that permit an assessment of essential characteristics of the personality of a natural person. Swiss data protection law provides an enhanced data protection level for personality profiles, similar to the protection of sensitive personal data. The draft of the revised DPA foresees that the term ‘personality profile’ shall be replaced by the term ‘profiling’, bringing a closer alignment to the corresponding definition provided for by the GDPR.

- **f** Data file: any set of personal data that is searchable by data subject. It is likely that this term will no longer be used under the revised DPA.

- **g** Controller of the data file: the controller of the data file is the private person or federal body that decides on the purpose and content of a data file (the draft of the revised DPA merely uses the term ‘controller’ instead, bringing a closer alignment to the corresponding term used in the GDPR).

As mentioned, it is likely that some terms will change under the revised data protection regime. In particular, it appears likely that ‘profiling’ will replace the term ‘personality profiles’ and the concepts of ‘data file’ and ‘controller of the data file’ will no longer be used in the...
revised DPA. However, as mentioned above, the suggested amendments of the DPA are still subject to parliamentary discussions and it is thus too early to give conclusive indications as to the revised wording of the DPA.

ii General obligations for data handlers

Anyone processing personal data must observe the following general obligations.\(^{18}\)

**Principle of good faith**

Personal data must be processed in good faith. It may not be collected by misrepresentation or deception.

**Principle of proportionality**

The processing of personal data must be proportionate. This means that the data processing must be necessary for the intended purpose and reasonable in relation to the infringement of privacy. Subject to applicable regulations on the safekeeping of records, personal data must not be retained longer than necessary.

**Principle of purpose limitation**

Personal data may only be processed for the purpose indicated at the time of collection, unless the purpose is evident from the circumstances or the purpose of processing is provided for by law.

**Principle of transparency**

The collection of personal data, and in particular the purposes of its processing, must be evident to the data subject concerned. This principle does not always lead to a specific disclosure obligation, but it will be necessary to give notice of any use of personal data that is not apparent to the data subject from the circumstances. For example, if personal data are collected in the course of concluding or performing a contract, but the recipient of the personal data intends to use the data for purposes outside the scope of the contract or for the benefit of third parties, then those uses of the personal data must be disclosed to the data subject.

**Principle of data accuracy**

Personal data must be accurate and kept up to date.

**Principle of data security**

Adequate security measures must be taken against any unauthorised or unlawful processing of personal data, and against intentional or accidental loss, damage to or destruction of personal data, technical errors, falsification, theft and unlawful use, unauthorised access, changes, copying or other forms of unauthorised processing. If a third party is engaged to process personal data, measures must be taken to ensure that the third party processes the personal data according to the given instructions and that the third party implements the necessary adequate security measures.

---

\(^{18}\) Articles 4, 5 and 7 DPA.
Detailed technical security requirements for the processing of personal data are set out in the DPO.

**Principle of lawfulness**

Personal data must be processed lawfully. This means that the processing of personal data must not violate any Swiss legislative standards, including any normative rules set forth in acts other than the DPA that directly or indirectly aim at the protection of the personality rights of a data subject.

**Processing personal data does not necessarily require a justification**

According to the Swiss data protection regime, the processing of personal data does not **per se** constitute a breach of the privacy rights of the data subjects concerned. Accordingly, processing in principle only requires a justification if it unlawfully breaches the privacy of the data subjects (Article 12 Paragraph 1 in relation to Article 13 DPA).

In general, no justification for the processing of personal data is required if the data subjects have made the data in question generally available and have not expressly restricted the data processing (Article 12 Paragraph 3 DPA). In contrast, a justification is required particularly if the processing violates one of the general data protection principles of the DPA outlined above, if the personal data is processed against the data subjects’ express will, or if sensitive personal data or personality profiles are disclosed to third parties for such third parties’ own purposes (Article 12 Paragraph 2 DPA).

In cases where a justification is required for a specific data processing, possible forms of justification are (1) consent by the data subject concerned, (2) a specific provision of Swiss (federal, cantonal and municipal) law that provides for such data processing, or (3) an overriding private or public interest\(^*\) in the data processing in question (Article 13 Paragraph 1 DPA).

According to Article 13 Paragraph 2 DPA, an overriding private interest of the data handler shall be considered in particular if he or she:

\(a\) processes personal data in direct connection with the conclusion or the performance of a contract and the personal data in question are the data of one of the contractual parties;

\(b\) competes for business with, or wants to compete for business with, another person and processes personal data for this purpose without disclosing the data to third parties for such third parties’ own purposes;

\(c\) processes data that are neither sensitive personal data nor a personality profile to verify the creditworthiness of another person, and discloses the data to third parties for the third parties’ own purposes only if the data are required for the conclusion or the performance of a contract with the data subject;

\(d\) processes personal data on a professional basis exclusively for publication in the edited section of a periodically published medium;

---
\(^*\) The public interest justification must exist from a Swiss perspective. However, this does not only include Swiss public interests. Supporting foreign concerns – depending on the circumstances – may also qualify as a public interest from a Swiss perspective. This needs to be checked on a case-by-case basis.
processes personal data for purposes that are not related to a specific person, in particular research, planning or statistics, and the results are published in a manner that does not permit the identification of the data subjects; or

collects personal data about a person who is a public figure to the extent that the personal data relates to the role of the person as a public figure.

The fact that a data handler has one of the above-listed interests in processing personal data does not mean per se that the data handler has an overriding interest in processing the personal data. The interest of the data handler in processing the personal data must always be weighed against the interest of the data subject in being protected against an infringement of his or her privacy. Only in situations where the interest of the data handler outweighs the interest of the data subject is the processing of personal data justified by the overriding interest of the data handler.

Consent

Under Swiss data protection law, processing of personal data does not require consent of the data subject concerned in all instances. As mentioned above, consent of the data subject may constitute a possible justification for a data processing that would otherwise be unlawful (e.g., because of an infringement of the principles outlined above, or in the event of a disclosure of sensitive personal data or personality profiles to third parties for such third parties’ own purposes). To the extent that the legality of data processing is based on the consent of the data subject concerned, the consent is only valid if (1) it is given voluntarily upon provision of adequate information and, (2) in case of processing of sensitive personal data or personality profiles, it is given expressly (Article 4 Paragraph 5 DPA).

Registration

Controllers of data files that regularly process sensitive personal data or personality profiles, or regularly disclose personal data to third parties (including affiliates), must register their data files with the Commissioner before they start processing the data (Article 11a DPA). The Commissioner maintains a register of data files that have been registered in this manner that is accessible online. If a controller is required to register, it becomes subject to additional documentary obligations. There are several exceptions to the duty to register data files. Inter alia, no registration is required if the controller of the data file is obliged by Swiss law to process the data in question (e.g., in the case of an employer processing employee data for Swiss social security purposes) or has nominated its own independent data protection officer monitoring the data protection compliance of the data controller. Several further exceptions are set forth in Article 11a Paragraph 5 DPA and Article 4 Paragraph 1 DPO.

The draft of the revised DPA foresees that the registration duty shall be repealed and replaced with a new documentation requirement for both controllers and processors similar to the records of processing activities according to Article 30 GDPR.

---

20 See Article 12 Paragraph 2 Letter (c) DPA.
iii Technological innovation and privacy law

Automated profiling and data mining

The legality of automated profiling and data mining is doubtful under Swiss data protection law, as such practices inherently involve the use of personal data for a range of purposes, some of which may not have been disclosed when the personal data was collected. Hence, such practices may constitute an unlawful breach of privacy because of an infringement of the principles of transparency, purpose limitation and proportionality unless justified by law, an overriding public or private interest or consent.

Cloud computing

Cloud computing raises various data protection issues. The Commissioner has issued a guide pointing out the risks and setting out the data protection requirements when using cloud computing services.21

In particular, the processing of personal data may only be assigned to a cloud service provider if the assignment is based on an agreement or on the law, if the personal data is processed by the cloud service provider only in the manner permitted for the assignor, and if the assignment is not prohibited by a statutory or contractual duty of confidentiality (Article 10a Paragraph 1 DPA). Furthermore, the assignor must ensure that the cloud service provider guarantees data security (Article 10a Paragraph 2 DPA). The assignor must in particular ensure that the cloud service provider preserves the confidentiality, availability and integrity of the personal data by taking adequate measures against unauthorised processing through adequate technical and organisational measures (see Article 7 DPA and Article 8 et seq. DPO). Additionally, if cloud computing services involve disclosures of personal data abroad, the specific requirements for transborder data flows must be complied with (see Section IV). Finally, the assignor must also ensure that, despite the use of a cloud service provider, the data subjects may still exercise their right to information (Article 8 DPA), and may demand deletion or correction of data in accordance with Article 5 DPA.

Big data

Big data offers manifold opportunities for social and scientific research and for businesses, but at the same time, it may threaten privacy rights if the processed data is not or not adequately anonymised. The DPA is not applicable to fully and completely anonymised data. In contrast, if the processing of big data involves the processing of data that has not been fully and completely anonymised (e.g., because it can be ‘de-anonymised’ at a later stage by merging different data files), the right to privacy and the protection of personal data need to be ensured. The use of big data that is not entirely anonymised and the general data protection principles of the DPA are potentially conflicting, particularly with regard to the principles of purpose limitation, proportionality and transparency (see Section III.ii).

Cookies
Since 2007, the use of cookies has been regulated in Article 45c Letter (b) of the Telecommunications Act of 30 April 1997.\textsuperscript{22} According to this Article, website operators have to inform users about the use of cookies and its purpose. Furthermore, they need to explain how cookies can be rejected (i.e., how cookies can be deactivated in the user’s browser). Switzerland basically follows the opt-out principle.

Drones
In Switzerland, in general, drones of up to 30 kilograms do not require a specific permit, as long as they do not overfly crowds of people and provided that the ‘pilot’ has visual contact with the drone at all times.\textsuperscript{23} Nowadays drones are usually equipped with cameras. As a result, people using drones need to comply with data protection regulations as soon as they view or record identified or identifiable persons. To the extent that such viewing or recording constitutes an unlawful breach of the privacy of the data subjects concerned, it needs to be justified either by the consent of the injured party, by an overriding private or public interest or by law (Article 13 Paragraph 1 DPA).\textsuperscript{24}

iv Specific regulatory areas
Processing of employee data in general
Article 328b of the Swiss Code of Obligation (CO) applies in addition to the DPA to the processing of personal data of employees.

According to Article 328b CO, the employer may process personal data concerning an employee only to the extent that the personal data concerns the employee's suitability for his or her job or is necessary for the performance of the employment contract. Article 328b CO is mandatory, and any deviation from this provision to the disadvantage of the employee is null and void (Article 362 CO).\textsuperscript{25}

Furthermore, Article 26 of Ordinance 3 to the Employment Act\textsuperscript{26} prohibits the use of systems that monitor the behaviour of employees, except if the monitoring systems are necessary for other legitimate reasons (e.g., quality control, security requirements, technical reasons) and provided that the systems do not impair the health and mobility of the

\textsuperscript{22} Classified compilation (SR) 784.10, last amended as of 1 September 2017.
\textsuperscript{23} Ordinance of the Federal Department of the Environment, Transport, Energy and Communications on special categories of aircraft of 24 November 1994, last amended as of 19 July 2017, classified compilation (SR) 748.941.
\textsuperscript{24} Article 179 quater CC is also relevant in this context, which states that a person who, without consent, observes with a recording device or records with an image-carrying device information from the secret domain of another person or information from the private domain of another person that is not readily available to everyone is criminally liable; see also Commissioner, ‘Video surveillance with drones by private persons’, available at https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/technologien/videoueberwachung/videoueberwachung-mit-drohnen-durch-private/videoueberwachung-mit-drohnen-durch-private.html (status 2014; in German; no English version available; last visited on 21 July 2018).
\textsuperscript{25} Some legal authors, however, are of the opinion that an employee may specifically and unilaterally consent (i.e., not in the employment contract or in any other agreement with the employer) to a processing of personal data that goes beyond Article 328b CO.
\textsuperscript{26} Ordinance 3 to the Employment Act (Healthcare) of 18 August 1993, last amended as of 1 October 2015, classified compilation (SR) 822.113.
employees concerned. If monitoring is required for legitimate reasons, it must at all times remain proportionate (i.e., limited to the extent absolutely required) and the employees must be informed in advance about the use of monitoring systems. Permanent monitoring is in general not permitted.

The Commissioner has issued specific guidelines with respect to the processing of employee data.27

Monitoring of internet and email use by employees
As regards monitoring of internet and email use by employees in particular, the following requirements apply:

a. the employer shall issue a ‘use policy’ that describes the permitted uses the employee may make of company internet and email resources;
b. constant individual analysis of log files is not allowed;
c. permanent anonymous analysis of log files and random pseudonymised analysis are admissible to verify whether the use policy is complied with;
d. individual analysis of log files is only allowed if the employee has been informed in advance of this possibility (e.g., in a ‘monitoring policy’) and if misuse has been detected or there is a strong suspicion of misuse; and

e. the monitoring policy must particularly indicate the possibility of an individual analysis, the possibility of forwarding the analysis to the HR department in the event of misuse and any possible sanctions.

As a general rule, employers shall not read any employee emails that have private content (even if misuse has been established). In the event of specific suspicion of a criminal offence, evidence may, however, be saved, and the employer may refer to the criminal prosecution authorities for further prosecution.

Whistle-blowing hotlines
The use of whistle-blowing hotlines is not specifically regulated by the DPA or the CO. Hence, the general rules, in particular on data and employee protection, apply. In a nutshell and from a DPA and CO perspective, whistle-blowing hotlines can be used if certain minimum requirements are met, such as, inter alia:

a. the transparent informing of employees, contractors, etc., about the existence of the whistle-blowing hotline;
b. the informing of relevant employees, contractors, etc., of allegations about them contained in a specific whistle-blowing report, unless there is an overriding interest not to do so in order to protect the ensuing investigations or the reporting person;
c. adequate safeguards to protect the data subjects from false or slanderous accusations; and

d. strong state-of-the-art security measures.

However, it is important to verify compliance on an individual basis before implementing a whistle-blowing hotline. In particular, and unless an exception applies, whistle-blowing hotlines (and the underlying data files, respectively) may require prior registration with the Commissioner (see Section III.ii), and in the event of transfers abroad, specific requirements must be met (see Section IV). Furthermore, and in particular in a cross-border context, whistle-blowing hotlines may be impacted by blocking statutes (see Section VI).

**Bring your own device (BYOD)**

Using BYOD causes data protection concerns because of the difficulty in separating private and business data. The Commissioner recommends respecting the following rules while using BYOD:

- a. establish clear use regulations about what is allowed and what is prohibited;
- b. maintain a separation of business and private data (both technical and logical);
- c. ensure data security (e.g., through encryption or passwords);
- d. establish clear regulations on where the business data are stored;
- e. use of employees’ own devices must be approved in advance by a person responsible within the company; and
- f. establish clear regulations regarding access to the device by the employer.  

**IV INTERNATIONAL DATA TRANSFER AND DATA LOCALISATION**

Any disclosure of personal data from Switzerland to countries abroad must comply with the DPA. A disclosure of data abroad occurs when personal data are transferred from Switzerland to a country outside of Switzerland or when personal data located in Switzerland are accessed from outside of Switzerland. The DPA prohibits a disclosure of personal data abroad if the transfer could seriously endanger the personality rights of the data subjects concerned. Such a danger may in particular occur if the personal data are disclosed to a country whose legislation does not guarantee an adequate protection of personal data.

The Commissioner has published a (non-binding) list of countries that provide an adequate data protection level with respect to individuals. As a rule, EU and EEA countries are considered to provide an adequate data protection level relating to individuals.

With respect to data transfers to non-EU or non-EEA countries, it is necessary to check on a case-by-case basis whether the country provides an adequate level of data protection with respect to personal data pertaining to individuals and legal entities. The same applies strictly speaking for transfers of personal data relating to legal entities to EU or EEA countries.

---

28 Commissioner, ‘Bring Your Own Device (BYOD)’ (available at https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/arbeitsbereich/bring-your-own-device--byod-.html; in German; no English version available; last visited on 21 July 2018).
30 It can, in our view, be reasonably argued that the fact that the EU data protection provisions (GDPR) do not specifically protect personal data pertaining to legal entities does not per se result in an absence of adequate protection in EU or EEA member states. The protection for such data may also be adequate based on other legislation of EU or EEA member states. Furthermore, the transfer of personal data pertaining to legal entities does not necessarily seriously endanger the legal entity’s personality rights.
If personal data are to be transferred to a country that does not provide an adequate data protection level for the personal data being transferred, the transfer may only occur if (Article 6 Paragraph 2 DPA):

- a sufficient safeguards, in particular contractual clauses (typically EU Model Contract Clauses adapted to Swiss law requirements), ensure an adequate level of protection abroad;
- b the data subject has consented in an individual specific case;
- c the processing is directly connected with the conclusion or the performance of a contract and the personal data are that of a contractual party;
- d disclosure is essential in specific cases to either safeguard an overriding public interest, or for the establishment, exercise or enforcement of legal claims before the courts;
- e disclosure is required in the specific case to protect the life or the physical integrity of the data subject;
- f the data subject has made the data generally accessible and has not expressly prohibited its processing; or
- g disclosure is made within the same company or the same group of companies, provided those involved are subject to data protection rules that ensure an adequate level of protection (i.e., that have adopted binding corporate rules, BCR).

In case of data transfer justified under Letter (a) and (g) above, the Commissioner must be informed in advance (i.e., before the transfer takes place) about the safeguards that have been taken or the BCR that have been adopted. If the safeguards consist of EU Model Contract Clauses adapted to Swiss law requirements or other contractual clauses explicitly accepted by the Commissioner, then it is sufficient to inform the Commissioner that such clauses have been entered into, and there is no need to actually submit the clauses to the Commissioner for review. As regards information about BCR, it is common practice to submit a copy of the rules to the Commissioner.

On 11 January 2017, the Swiss Federal Council announced the establishment of the Swiss–US Privacy Shield. This framework is separate from – but closely resembles – the EU–US Privacy Shield (which was formally adopted by the European Commission on 16 July 2016 and predates the Swiss–US Privacy Shield). It replaces the former Swiss–US Safe Harbor Framework and purports to facilitate the transfers of personal data from Switzerland to the United States. Companies based in the United States have been able to self-certify under the Swiss–US Privacy Shield since 12 April 2017. For a company certified under the Swiss–US Privacy Shield an adequate level of data protection is deemed to exist for the personal data covered by the certification. Hence personal data may be transferred from Switzerland to a company based in the United States that is certified under the Swiss–US Privacy Shield even if none of the exceptions set forth in Article 6 Paragraph 2 DPA apply. As mentioned


32 The dedicated Privacy Shield Framework website sets up this process: www.privacyshield.gov/welcome (last visited on 21 July 2018). It also allows any interested person to consult the list of certified companies: www.privacyshield.gov/list.
above, the Swiss–US Privacy Shield is separate from the EU–US Privacy Shield. For transfers from Switzerland to the United States, the certification under the Swiss–US Privacy Shield is relevant and a certification only under the EU–US Privacy Shield is not sufficient.

V COMPANY POLICIES AND PRACTICES

According to Article 11 Paragraph 1 DPA, the private controller 33 of an automated data file subject to registration under Article 11a Paragraph 3 DPA that is not exempted from the registration requirement under Article 11a Paragraph 5 Letters (b)–(d) DPA shall issue a processing policy that describes in particular the internal organisation, data processing and control procedures, and that contains documentation on the planning, realisation and operation of the data file and the information technology used. This policy must be updated regularly and made available upon request to the Commissioner.

Other than in the aforementioned case, the DPA does not explicitly require private personal data handlers to put in place any specific policies as regards the processing of personal data. However, for private personal data handlers to effectively ensure compliance with substantive and formal data protection requirements, it has become best practice for large and medium-sized companies to adopt and implement various policies in this area. In particular, the following policies (either in separate or combined documents) are recommended:

a a policy regarding the processing of job applicant and employee personal data (including a policy that governs the use by employees of the company’s information technology resources, monitoring by the employer of employees’ use of those resources and possible sanctions in the event of misuse, rules on BYOD, etc.);

b a policy regarding the processing of customer personal data;

c a policy regarding the processing of supplier personal data;

d a whistle-blowing policy;

e a policy or privacy notice for collecting and processing personal data on a company’s websites;

f a policy on data and information security (qualification of data according to risk, required measures per risk category, access rights, procedures in the event of data breaches, internal competence, etc.); and

g a policy on archiving of personal data and record-keeping (including guidelines on how long different categories of data must be stored).

In contrast to other countries’ legislation, the DPA does not require private data handlers to appoint a data protection officer. For this reason, and until a few years ago, companies’ data protection officers have not played a very important role in Switzerland compared with their role in other countries. However, in the past few years, more and more medium-sized and large companies domiciled in Switzerland have chosen to appoint a data protection officer who independently monitors internal compliance with data protection regulations and maintains a list of the data files of the company in question. In fact, appointing such a data protection officer is one way for private data controllers to avoid having to register data files with the Commissioner that otherwise would have to be registered under the current regime

33 Federal public controllers of data files have a similar obligation to issue a processing policy for automated data files that contain sensitive personal data or personality files, are used by two or more federal bodies, are disclosed to third parties or are connected to other data files (see Article 21 DPO).
(see Article 11a Paragraph 3 DPA in relation to Article 11a Paragraph 5 Letter (e) DPA; see also Section III.ii). Currently, over 1,000 companies have notified the Commissioner of their appointment of an independent data protection officer.

BCR ensuring an adequate level of protection of personal data on a group-wide level facilitate the cross-border disclosure of personal data among group companies (see Section IV). Despite this fact, and until recently, BCR have not been used very frequently in Switzerland.

VI DISCOVERY AND DISCLOSURE

In Switzerland, the taking of evidence constitutes a judicial sovereign function of the courts rather than of the parties. Therefore, taking of evidence for a foreign state court or for foreign regulatory proceedings constitutes an act of a foreign state. If such acts take place in Switzerland, they violate Swiss sovereignty and are prohibited by Article 271 of the Swiss Criminal Code of 21 December 1937 (CC) unless they are authorised by the appropriate Swiss authorities or are conducted by way of mutual legal assistance proceedings (a blocking statute). A violation of Article 271 CC is sanctioned with imprisonment of up to three years or a fine of up to 540,000 Swiss francs, or both. It is important to note that transferring evidence outside Switzerland for the purposes of complying with a foreign country’s order requiring the production of evidence does not prevent an application of Article 271 CC. Moreover, Switzerland does not accept ‘voluntary’ production of evidence even if foreign procedural laws require such production. Therefore, evidence may only be handed over to foreign authorities lawfully by following mutual legal assistance proceedings or by obtaining authorisation from the competent Swiss authorities. If one is requested to produce evidence in a foreign court or in regulatory proceedings by way of pending mutual legal assistance proceedings, the DPA does not apply to the production (Article 2 Paragraph 2 Letter (c) DPA). As a consequence, and in particular, evidence containing personal data may in such cases be disclosed abroad to foreign parties or authorities located in countries without adequate protection of personal data without having to comply with the restrictions set forth in Article 6 DPA.

In addition to Article 271 CC, the blocking statute in Article 273 CC prohibits industrial espionage of manufacturing and business secrets by foreign official agencies, foreign organisations, foreign private enterprises or their agents. Accordingly, manufacturing and business secrets with sufficient connection to Switzerland may only be released or communicated abroad when:

a. the owner of the secret relinquishes its intent to keep the information secret;

b. the owner of the secret agrees to disclose this information;

34 The DPA also does not apply to pending Swiss civil proceedings, pending Swiss criminal proceedings and pending Swiss proceedings under constitutional or under administrative law, with the exception of administrative proceedings of first instance (see Article 2 Paragraph 2 Letter (c) DPA).

35 In contrast, producing and taking evidence in purely private foreign arbitral proceedings is not subject to Article 271 CC and therefore do not require that the parties follow the requirements of mutual legal assistance proceedings. However, as the DPA fully applies to the processing of personal data in foreign-based private arbitral proceedings, any cross-border disclosure must comply with the requirements set forth in Article 6 DPA (see Section IV). For more details and exceptions, see Jürg Schneider, Ueli Sommer, Michael Cartier, in Catrien Noorda, Stefan Hanloser (eds), E-Discovery and Data Privacy: A Practical Guide, Kluwer Law International BV, 2011, Chapter 5.25, Switzerland.
c all third parties (who have a justifiable interest in keeping the information secret) consent to such a disclosure;

d Switzerland has no immediate sovereign interest in keeping the information secret; and

e all requirements set forth by the DPA (in particular as regards cross-border transfers) are complied with.

However, Article 273 CC does not apply in cases in which Swiss authorities have granted mutual legal assistance and disclosure takes place in accordance with the proceedings. Contrary to Article 271 CC, Article 273 CC can also be violated by activities taking place outside Switzerland.

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

The Commissioner supervises compliance of both federal bodies and private persons (individuals and legal entities) with the DPA, DPO and other federal data protection regulations. The Commissioner fulfils these tasks independently without being subject to the directives of any authority.

For this purpose, the Commissioner may investigate cases either on his or her own initiative or at the request of a third party. The Commissioner may request the production of files, obtain information and request that a specific instance of data processing is demonstrated to him or her. If such an investigation reveals that data protection regulations are being breached, the Commissioner may make recommendations as to how the method of data processing shall be changed or that the data processing activity shall be stopped. If such a recommendation is not complied with, the Commissioner may initiate proceedings leading to a formal decision on the matter.

In the case of recommendations to federal bodies, the Commissioner may refer the case to the competent department or the Swiss Federal Chancellery for a formal decision. Both the Commissioner and any persons concerned by such a decision may file an appeal against the decision with the Swiss Federal Administrative Court. The appeal decision can be appealed to the Swiss Federal Supreme Court.

In the case of recommendations to private persons, the Commissioner may refer the case to the Swiss Federal Administrative Court for a decision. Both the Commissioner and the addressee of such a decision may file an appeal against the decision with the Swiss Federal Supreme Court.

The Commissioner does not have the power to issue any fines. However, based on Article 34 DPA, the competent criminal judge may, upon complaint, sanction private persons with a fine of up to 10,000 Swiss francs if they have wilfully breached their obligations to:

a provide information upon request of the data subject concerned under Article 8 DPA;

b provide information on the collection of sensitive personal data and personality profiles under Article 14 DPA;

36 The processing of personal data by cantonal and communal bodies is regulated by cantonal law. Each canton has a cantonal data protection authority, be it a cantonal data protection officer or a commission competent for cantonal and communal data protection matters. Some cantons have jointly appointed an inter-cantonal data protection authority.
c inform the Commissioner about the safeguards and data protection rules in relation to a transfer of personal data abroad under Article 6 Paragraph 3 DPA;  
d register a database with the Commissioner; or  
e cooperate with the Commissioner (Article 34 DPA).

Furthermore, anyone who without authorisation wilfully discloses confidential, sensitive personal data or personality profiles that have come to his or her knowledge in the course of his or her professional activities is, upon complaint, liable to a fine of up to 10,000 Swiss francs (Article 35 DPA in connection with Article 106 Paragraph 1 of the CC).  

ii Recent enforcement cases

The Swiss Federal Supreme Court’s decision of 12 January 2015 in connection with the tax dispute between certain Swiss banks and the United States is particularly noteworthy. Based on the right of access set forth in Article 8 DPA, the Court obliged a Swiss bank to provide its employees with copies of all documents transferred to the US Department of Justice in April 2012 containing their personal data.  

As regards the processing of employee personal data, the Swiss Federal Supreme Court held in 2013 that the monitoring of an employee’s use of email and internet that lasted for three months and included taking regular screenshots was illegal and not proportionate. Moreover, the monitoring was not backed by an internal policy that permitted monitoring under specific, transparently disclosed circumstances.

More recently, several court decisions have been rendered regarding data protection issues in connection with the granting of access to official documents based on the Swiss Federal Freedom of Information Act of 17 December 2004. In three parallel rulings dated 23 August 2016, the Swiss Federal Administrative Court decided on the scope of Article 19 Paragraph 4 Letter (a) and (b) DPA, according to which federal bodies shall refuse or restrict disclosure of documents, or make such disclosure subject to conditions if (1) essential public interests or clearly legitimate interests of a data subject so require; or (2) statutory duties of confidentiality or special data protection regulations so require. In the case at hand, communal bodies requested access to documents from a closed bid-rigging proceeding investigated and decided by the Swiss Competition Commission in an attempt to collect evidence for civil follow-on actions. The Swiss Federal Administrative Court held that victims of anticompetitive conduct may be granted such access to information under the conditions

---

37 According to the latest statistics published by the Swiss Federal Statistical Office, only 43 offences in the sense of Article 34 and Article 35 DPA have been reported during 2009 to 2015. The published statistics neither indicate whether the sanctions relate to Article 34 or Article 35 DPA nor mention the amount of fines that have been imposed. Furthermore, the published statistics may be incomplete and the actual number of sanctions may be higher.

38 Swiss Federal Supreme Court decisions dated 12 January 2015, 4A_406/2014; 4A_408/2014 (BGE 141 III 119).

39 Swiss Federal Supreme Court decision dated 17 January 2015 (BGE 139 II 7).

40 Classified compilation (SR) 152.3, last amended as of 19 August 2014.

that the information does not contain business secrets in the sense of Article 25 of the Swiss Federal Cartel Act of 6 October 1995 (ACart)\(^{42}\) and does not contain information provided by leniency applicants in the sense of Article 49a Paragraph 2 ACart.

On 11 May 2017, the Swiss Federal Administrative Court published a leading case dated 18 April 2017 relating to personality profiles and retrievability of personal data via search engines.\(^{43}\) The decision, which concerns a case of the Commissioner against a Swiss economic information platform and credit agency, is final and binding as none of the parties appealed against said decision. The Swiss Federal Administrative Court came to the conclusion that personal data that in combination reveals an essential part of the personality of a data subject and that is not relevant in assessing the creditworthiness of the person in question may not be published without the consent of the data subject concerned. The Commissioner’s claim that the economic information platform and credit agency’s data relating to persons registered in the commercial registry should only be retrievable with search engines in the same manner as data of the official Swiss Federal Commercial Registry was rejected (search engines, in particular Google, only show search results for the Swiss Commercial Registry (i.e., www.zefix.ch) if the search name and also the term ‘Zefix’ are entered into the search tool). The Swiss Federal Administrative Court stated that the economic information platform and credit agency only has limited influence on the publication of search results on search engines. Also, the Swiss Federal Administrative Court pointed out that the possibility of finding data via search engines may have positive effects from a data protection perspective as it increases transparency.

Lastly, the European Court of Human Rights (ECHR), in a ruling of 18 October 2016, overruled a decision of the Swiss Federal Supreme Court in the field of publicly regulated accident insurance. The Swiss Supreme Court had previously ruled that accident insurance companies could lawfully conduct secret surveillance of the candidates for, or beneficiaries of, insurance benefits, despite the absence of a sufficiently detailed legal basis. Subsequent to the ECHR ruling, the Swiss Federal Supreme Court, on 14 July 2017, in line with the ECHR ruling, decided that, likewise, the federal social security office could not lawfully conduct secret surveillance of candidates for or beneficiaries of disability insurance. The Swiss parliament is currently drafting an amendment that provides sufficient legal basis for such surveillance by specifically setting out applicable requirements and conditions.

### iii Private litigation

Any person may request information from the controller of a data file as to whether personal data concerning them is being processed (Article 8 Paragraph 1 DPA). This ‘right to information’ includes information about:

- **a** the source of the personal data;
- **b** the purpose of and, if applicable, the legal basis for, the processing as well as the categories of the personal data processed;
- **c** the other parties involved in the processing; and
- **d** the data recipient concerned (Article 8 Paragraph 2 DPA).

---

\(^{42}\) Classified compilation (SR) 251, last amended as of 1 December 2014.

This information must normally be provided in writing, in the form of a printout or a photocopy, and is in principle free of charge (a fee of up to 300 Swiss francs may be levied in exceptional cases outlined in Article 2 DPO). Any data subject may also request that incorrect data be corrected (Article 5 Paragraph 2 DPA).

In addition, data subjects have ordinary judicial remedies available under civil law to protect their personality rights (Article 15 DPA in relation to Article 28–28l of the Swiss Civil Code). Data subjects may in particular request:

- that data processing be stopped;
- that no data be disclosed to third parties;
- that the personal data be corrected or destroyed;
- compensation for moral sufferings; and
- payment of damages or the handing over of profits.

However, as regards claims for damages, it is in practice often very difficult for a data subject to prove actual damage based on privacy infringements.

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

The territorial scope of application of the DPA is very broad. The DPA not only applies to the processing of personal data in Switzerland (which is the most common trigger), but – depending on the circumstances – may also apply to the processing of personal data that takes place abroad. In fact, based on an international convention or based on Article 129 Paragraph 1 and Article 130 Paragraph 3 PILA, a data subject may in some instances have the option to file an action in a Swiss court for infringement of his or her personality rights and ask the competent court to apply Swiss law even if no processing activity has taken place in Switzerland (see Article 139 PILA).44 Based on the foregoing, foreign organisations should review compliance with the DPA even if they do not process any personal data in Switzerland or even if they do not have any presence in Switzerland if there is a possibility that data subjects may file a claim in Switzerland and ask for the application of the DPA.

As regards foreign organisations with personal data processing operations in Switzerland (e.g., through a branch office, an affiliate or a third-party service provider), compliance with the requirements on international data transfers is another important topic if a cross-border exchange of personal data is involved (e.g., in the context of centralised HR and customer relationship management systems – see Section IV). Moreover, if a foreign organisation transfers or discloses personal data to Switzerland for the first time, additional or new obligations for the processing of the personal data may be created that did not exist beforehand.45 We therefore strongly recommend verifying compliance with the DPA before disclosing or transferring any personal data to Switzerland, before starting to process personal

44 This, however, does not apply to public law provisions of the DPA (such as the obligation to register a data file with the Commissioner or to inform the Commissioner of a transfer abroad) as such rules are governed by the principle of territoriality and only apply to facts that take place in Switzerland.

45 Such as, for example, an obligation to register a data file with the Commissioner, or there may be instances where data that before their transfer or disclosure to Switzerland were not subject to specific data protection regulations suddenly becoming subject to the data protection regulations set forth in the DPA and the DPO because of the fact that the DPA and DPO currently also apply to the processing of personal data pertaining to legal entities (even if, at a later stage, the data are transferred abroad from Switzerland again).
data in Switzerland (whether on one’s own or by using group companies or third-party service providers), or before cross-border exchanges of personal data in the context of a group of companies or otherwise.

IX CYBERSECURITY AND DATA BREACHES

Article 7 DPA and Articles 8–12 DPO set out the general security requirements applicable to the processing of personal data. Additionally, the Commissioner has issued a guide pertaining to technical and organisational measures to be taken when processing personal data.46

Neither the DPA nor the DPO currently explicitly require data handlers to notify the Commissioner (nor any other Swiss authority) or data subjects of any suspected or actual personal data breaches (note that this is likely to change under the revised DPA).47 However, data handlers may indeed have a duty to inform data subjects concerned based on the principles of transparency and good faith. Data handlers may in certain circumstances also have a contractual obligation to notify data subjects of any suspected or actual personal data breaches.48 In the event that a large number of data subjects are affected, the principles of transparency and good faith may very exceptionally even result in a duty to report the incident publicly. This may in particular be the case if the data subjects concerned cannot be informed individually and there is a high probability that damages will occur if the incident is not publicly reported. Whether an obligation to notify data subjects exists (be it individually, through public reporting, or both) must be checked on a case-by-case basis.

In Switzerland, the cantons are generally responsible for the prosecution of misuse of information and communication technology. To fight cybercrime more efficiently, the Swiss Confederation and the cantons entered into an administrative agreement in 2001, empowering the federal authorities to assume certain responsibilities in this area. On 1 January 2014, the Swiss national coordination unit to fight internet crime, the Cybercrime Coordination Unit Switzerland (CYCO), commenced its activities.49 CYCO conducts an initial analysis of incoming reports, secures the relevant data and then forwards the matter to the competent law enforcement agencies in Switzerland and abroad.

46 ‘Guide for technical and organisational measures’ (status as of February 2016; https://www.edoeb.admin.ch/dam/edoeb/en/dokumente/2016/02/leitfaden_zu_dem_technischendes_organisatorischenmassnahmendesdate.pdf;download.pdf/guide_for_technicalandorganizationalmeasures.pdf, last visited on 21 July 2018). Additional security requirements apply to specific sectors such as, inter alia, the financial industry and the area of medical research. These additional requirements are set forth in separate legislative acts.

47 For certain specifically regulated areas, however, these duties may exist. This is the case, for instance, in the banking sector where regulatory requirements call for a notification in certain cases of data breaches (Circular 2008/21 – Operational Risks Banks, Annex 3, of the Swiss Financial Market Supervisory Authority – FINMA, available at: www.finma.ch/de/-/media/finma/dokumente/rundschreiben-archiv/finma-rs-2008-21---30-06-2017.pdf&sa=U&ved=0ahUKEwiZ8vetoovWAhUCibQKHcLuBeMQtggNMAQ&client=internal-uds-cse&usg=AFQjCNH1f9Man6e87Na3Uq4hV8R2iGy4g, last visited on 21 July 2018).

48 For example, a data handler may have an obligation to inform its customers about a data breach based on an explicit contractual obligation towards its customers or based on a general contractual duty of diligence. More information on CYCO is available at https://www.fedpol.admin.ch/fedpol/en/home/kriminalitaet/cybercrime.html (last visited on 21 July 2018).
On a Swiss federal level, the Reporting and Analysis Centre for Information Assurance (MELANI) was established in 2004. MELANI functions as a cooperation model, *inter alia*, between the Swiss Federal Finance Department and the Swiss Federal Defence Department. It serves private computers and internet users (in particular providing them with information about risks relating to the use of modern information and communication technologies) as well as selected providers of critical national infrastructures (such as banks and telecommunication services providers). MELANI has created various checklists and documentation regarding IT security. In 2008, MELANI established GovCERT.ch, the computer emergency response team (CERT) of the government, and the official national CERT of Switzerland, GovCERT.ch is a member of the Forum of Incident Response and Security Teams, and of the European Government CERTs group.

Finally, Switzerland ratified the Council of Europe Convention on Cybercrime of 2001 in 2011. The Convention entered into force for Switzerland on 1 January 2012 together with a minor amendment of the CC and the Swiss Federal Act on International Mutual Assistance in Criminal Matters of 20 March 1981.\(^{50}\)

## X OUTLOOK

The ongoing reform of the DPA is likely to lead to a tightening of the Swiss data protection regime. Based on the publication of the draft of the revised DPA,\(^{51}\) the following aspects are particularly noteworthy:

- **a** transparency in data processing is increased. In particular, private sector actors will have a duty to inform data subjects in the event of data collection and processing;
- **b** self-regulation shall be encouraged. Professional and business associations may prepare codes of conduct and submit them to the Commissioner for the delivery of an opinion;
- **c** the data controller will have to perform an impact assessment whenever it appears that the envisaged data processing may lead to an increased risk to the data subjects’ personality and fundamental rights, although some exceptions apply;
- **d** a duty to notify the Commissioner or even the data subjects in cases of breach of data protection will bind data controllers;
- **e** the present rules on personality profiles will be abolished. However, they will be replaced by new rules on profiling;
- **f** the draft introduces the concepts of privacy by design and privacy by default. Hence, data protection must take place from the outset (i.e., from the conception of the processing) and the least invasive settings must be applied by default;
- **g** the duty to declare data files to the Commissioner shall be abolished for private actors. Data controllers and data processors must, however, keep records of their processing activities;
- **h** personal data relating to legal entities shall no longer be protected under the DPA;
- **i** the Commissioner shall obtain greater powers and will in particular have the competence to render binding decisions on data controllers and processors; and
- **j** criminal sanctions for data protection misconduct will be increased significantly. In fact, fines of up to 250,000 Swiss francs may be levied in cases of intentional offences against certain provisions of the revised DPA.

\(^{50}\) Classified compilation (SR) 351.1, status as of 1 January 2013.

\(^{51}\) See footnote 6 for links to the draft of the revised DPA.
Moreover, the revision process will affect not only the DPA itself, but also many other laws, such as the CC, criminal procedure regulations and so forth.

The text that will eventually become law, may contain deviations from the published draft. It is nonetheless to be expected that the final revised DPA will include many of the changes suggested in the draft of the revised DPA. Entry into force of the new, revised DPA, which was initially expected to take place in 2018, should now unfold in two parts. A first part should enter into force in 2019, while the second part is tentatively expected to enter into force in 2020 (for further detail, see above Section II).
Chapter 24

TURKEY

Batu Kınıkoğlu, Selen Zengin and Kaan Can Akdere

I OVERVIEW

The protection of personal data is recognised as a fundamental right under Article 20(3) of the Constitution of the Republic of Turkey as of its amendment in 2010. Since the aforementioned Article requires that the principles and procedures regarding the protection of personal data shall be laid down in law; the constitutional guarantee for the protection of personal data is intended to manage the processing of personal data on a regulatory level. In this respect, Law on the Protection of Personal Data No. 6698 (the DP Law), which constitutes the main legislative instrument that specifies the principles and procedures concerning the processing and protection of personal data, has been published in the Official Gazette on 7 April 2016 and is in effect as of this date.

The data protection authority established by the DP Law, the Personal Data Protection Board (the Board), is currently active and has been regularly publishing secondary legislation of the DP Law as well as principle decisions and guidance documents concerning the application of the DP Law. Additionally, certain sector-specific data protection rules are scattered under sector-specific laws. For example, commercial economic communications are regulated under a different instrument and the administrative authority that supervises these communications is the Ministry of Trade and not the Board.

Because Turkey is currently not an EU country, in principle, EU’s General Data Protection Regulation (GDPR) is not directly applicable in Turkey. However, since the territorial scope of the GDPR applies where the personal data processing activities are related to the offering of goods or services to data subjects that are in the Union by a controller or processor not established in the Union, data controllers located in Turkey might be required to comply with the GDPR.

‘Data protection’ as a concept is becoming more and more topical in the country. The Board is continuing its work to create public awareness on the issue. On this endeavour, the

---

1 Batu Kınıkoğlu is a partner, Selen Zengin is an attorney and Kaan Can Akdere is a legal intern at BTS&Partners.
Board is organising seminars, sharing educational videos and publishing guidance documents with regards to the implementation of the principles and procedures set forth under the DP Law.

With regard to cybersecurity, the relevant legislation is still evolving. Cybersecurity rules are not consolidated under one legislative instrument but rather scattered under different sector-specific regulations. Entities practising in critical sectors such as telecommunications, energy, banking and finance, and insurance are generally subjected to cybersecurity or information-security requirements.

II THE YEAR IN REVIEW

Data protection has been an active legal area since the enactment of the DP Law, and 2018 has been no different. Two communiqués were published on the 10 March that are of high importance for private businesses: the Communiqué on the procedures and principles to be complied with when fulfilling the obligation to inform and the Communiqué on procedures and principles for data controller applications.

As of 9 July 2018, the Board has published five principle decisions that data controllers are obliged to follow and, as demonstrated by two data breach notifications published on its website, the Board is actively investigating data breaches that involve the personal data of Turkish citizens.

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

The main legislative instrument protecting the personal data of data subjects is the DP Law. Article 2 of the DP Law states that its provisions will be applicable to ‘natural persons whose personal data are processed and natural or legal persons who process such data wholly or partly by automatic means or by non-automated means which form part of a filing system’. Therefore, it can be said that the DP Law does not distinguish between the scope or type of data processing activities or the sector under which the data controller is operating; it applies to all.

Definitions of both ‘personal data’ and ‘processing of personal data’ are similar to their counterparts under the GDPR. ‘Personal data’ is defined as ‘any information relating to an identified or identifiable natural person’ and definition of ‘processing of personal data’ covers any operation performed upon personal data. The definition of ‘special categories of personal data’ includes data relating to race, ethnicity, political opinions, philosophical beliefs, religion, sect or other beliefs, appearance and dress, membership of associations, foundations or trade unions, health, sexual life, criminal convictions and security measures, and data relating to

4 Published in the Official Gazette No. 30356 and dated 10 March 2018.
5 Published in the Official Gazette No. 30356 and dated 10 March 2018.
7 Data breach notification made by Ticketmaster UK. Published on 29 June 2018: https://www.kvkk.gov.tr/Icerik/5244/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi.
biometrics and genetics. Notably, data relating to appearance and dress is not considered as a special category of personal data under the GDPR but is considered as such under the DP Law.

There is multiple secondary legislation of the DP Law that provides further specification on certain provisions of the DP Law. The secondary legislation that is most relevant to data controllers is as follows.

**Regulation on the Deletion, Destruction or Anonymisation of Personal Data**

The DP Law states that personal data shall be deleted, destroyed or anonymised either *ex officio* or upon the request of the data subject if the reasons necessitating their process cease to exist. This regulation provides further details on deletion, destruction and anonymisation of personal data.

**Regulation on the Registry of Data Controllers**

Under Article 16 of the DP Law, data controllers are required to register with the data controller registry. This regulation provides further details concerning the principles and procedures to be followed when fulfilling this obligation. Furthermore, the regulation brings two new titles: ‘data controller representative’ and ‘contact person’. People filling these positions will have significant duties with regards to conveying communication between data controllers and the Board.

**Communiqué on the Procedures and Principles to be Complied When Fulfilling the Obligation to Inform**

The communiqué provides further details concerning how data controllers will fulfil their obligation to notify the data subjects about the processing of their personal data. These details include which information must be given to data subjects and the means and methods of these notifications.

**Communiqué on Procedures and Principles for Data Controller Applications**

The Communiqué provides further details concerning how data subjects will direct their requests concerning their rights stated under the DP Law to data controllers and how data controllers will handle these requests.

**General obligations for data handlers**

The DP Law sets forth an array of obligations for data controllers. Some of these obligations can be listed as follows.

Processing personal data in accordance with principles and conditions stated under the DP Law

The most fundamental of data controller obligations is to comply with general principles stated under Article 4 for the processing of personal data and process personal data only when one of the conditions under Article 5 is met.

Principles to be followed when processing personal data include:

- conforming to the law and good faith principles;

---

8 Published in the Official Gazette No. 30224 and dated 28 October 2017.
9 Published in the Official Gazette No. 30286 and dated 30 December 2017.
being accurate and, if necessary, up to date;

processing for specified, explicit and legitimate purposes;

processing that is relevant, limited and proportionate to the stated purposes; and

storing data only for the time designated by the relevant legislation or necessitated by the purpose for which data is collected.

The conditions for lawful data processing stated under Article 5 are:

if none of the following conditions can be met, explicit consent of the data subject,

if processing is expressly permitted by any law;

if processing is necessary in order to protect the life or physical integrity of the data subject or another person where the data subject is physically or legally incapable of giving consent;

if it is necessary to process the personal data of parties of a contract, provided that the processing is directly related to the execution or performance of the contract;

if processing is necessary for compliance with a legal obligation which the controller is subject to;

if the relevant information is publicised by the data subject herself or himself;

if processing is necessary for the institution, usage, or protection of a right; and

if processing is necessary for the legitimate interests of the data controller, provided that the fundamental rights and freedoms of the data subject are not harmed.

Conditions for processing 'special categories of personal data' are provided under Article 6 and are more restricted.

It is prohibited to process special categories of personal data without obtaining the explicit consent of the data subject; however, special categories of personal data other than those relating to health and sexual life, may be processed without obtaining the explicit consent of the data subject if processing is permitted by any law.

Personal data relating to health and sexual life can only be processed without obtaining the explicit consent of the data subject for purposes of protection of public health, operation of preventive medicine, medical diagnosis, treatment and care services, planning and management of health services and financing by persons under the obligation of secrecy or authorised institutions and organisations.

iii Obligation to inform

According to Article 10 of the DP Law, data controllers are obliged to inform the data subjects about the following, at the point of collecting their personal data:

the identity of the data controller and, if any, its representative;

the purposes for which personal data will be processed;

the persons to whom processed personal data might be transferred and the purposes for the same;

the method and legal cause of collection of personal data; and

the rights set forth under Article 11 of the DP Law.

Explicit consent’ is defined as ‘Freely given, specific and informed consent’. Consent must be free (for example, consent must not be made conditional for the provision of a service), informed, limited to the relevant act of processing and have been given unambiguously by data subject acting in a way which leaves no doubt that the data subject agrees to the processing of his or her data.
Principles and procedures that must be followed when fulfilling this obligation are provided in detail under the Communiqué on the procedures and principles to be complied with when fulfilling obligation to inform (the Communiqué on the obligation to inform). For example, the Communiqué on the obligation to inform requires data controllers to inform data subjects and obtain their consent separately, and states that, when informing data subjects, a clear, simple and understandable wording must be used.

iv Registering with the data controller registry

Article 16 of the DP Law states that the data controllers are required to register with the Data Controller Registry (the Registry) before processing personal data. Although the Registry is not active as of July 2018, it is expected to open for registration soon.

The following information shall be provided to the Registry:

a identity and address information of the data controller and, if any, of its representative;
b the purposes for which personal data will be processed;
c the group or subject groups of persons of the data and explanations regarding data categories belonging to these persons;
d recipient or recipient groups to whom personal data may be transferred;
e personal data which is expected to be transferred abroad;
f measures taken for the security of personal data; and
g the maximum retention period for the purposes for which personal data are processed.

Principles and procedures regarding the obligation to register with the Registry are provided in detail under the Regulation on the Data Controller Registry. On an additional note, the Regulation requires data controllers resident in Turkey to appoint a contact person and register it with the Registry. The contact person shall be the ‘middleman’ that will carry out the communication with the data subjects and the data controller. Similarly, data controllers that are not resident in Turkey are expected to appoint a ‘data controller representative’, which can be either a real person who is a Turkish citizen, or a legal entity located in Turkey. This person shall be notified to the Registry during registration.

v Ensuring the security of personal data

Under Article 12 of the DP Law, data controllers are obliged to take all necessary technical and organisational measures to provide an appropriate level of security to:

a prevent unlawful processing of personal data;
b prevent unlawful access to personal data; and
c safeguard personal data.

What the phrase ‘all necessary technical and organisational measures’ actually means is not explicitly defined under the data protection legislation; however, the ‘Guidebook on Personal Data Security’ published by the Board11 provides guidance on what measures are expected from the data controllers to be taken.

What is more, the DP Law expects additional protective measures to be taken when handling special categories of personal data; these measures are specified under a principle

decision taken by the Board\textsuperscript{12} and include using cryptographic encryption measures, signing NDA agreements with the personnel and setting two-stage authentication systems over the information systems that contain personal data.

Additionally, data controllers are required to notify the relevant data subjects and the Board if personal data is obtained by others through unlawful means (e.g., a cyberattack or data leakage) as soon as possible.

vi Data subjects’ rights

As stipulated by Article 11 of the DP Law, every data subject has the following rights in relation to their personal data, which they may use by applying to the data controller. He or she may:

\begin{itemize}
\item[\textit{a}] learn whether their personal data have been processed,
\item[\textit{b}] request information as to processing if their data have been processed,
\item[\textit{c}] learn the purpose of processing of their personal data and whether data are used in accordance with their purpose,
\item[\textit{d}] learn the third parties those which their personal data have been transferred,
\item[\textit{e}] request rectification in case personal data are processed incompletely or inaccurately,
\item[\textit{f}] request deletion or destruction of their personal data within the framework of the conditions set forth under Article 7,
\item[\textit{g}] request notification of the operations made as per indents (e) and (f) to third parties to whom personal data have been transferred,
\item[\textit{h}] object to the occurrence of any result that is to their detriment by means of analysis of their personal data exclusively through automated systems,
\item[\textit{i}] request compensation for the damages in case they incur damages owing to unlawful processing of their personal data.
\end{itemize}

vii Specific regulatory areas

Electronic marketing

Electronic marketing communications are regulated under a separate regulation: Regulation on Commercial Communications and Electronic Commercial Communications.\textsuperscript{13} Commercial emails, text messages and outbound calls fall within the scope of the regulation and these electronic commercial messages are required to meet certain strict criteria to be regarded as lawful.

First, sending electronic commercial messages requires prior consent of the recipient. However, there are certain exceptions to the prior consent requirements such as if the message is sent to merchants and craftsman or the message relates to collection matters, debt reminders, information update, purchases, delivery and similar actions with respect to an ongoing subscription, membership or partnership, or contains information required by legislation to be sent to the recipient. The consent cannot be actively requested by sending

\begin{footnotesize}
\begin{itemize}
\item[\textsuperscript{12}] Personal Data Protection Board’s Decision No. 2018/10 dated 31/01/2018 on Adequate Security Measures to be Taken by Data Controllers When Processing Special Categories of Personal Data published on 7 March 2018: https://kvkk.gov.tr/Icerik/4110/2018-10.
\item[\textsuperscript{13}] Published in the Official Gazette No. 29417 and dated 15 July 2015.
\end{itemize}
\end{footnotesize}
an electronic communication to the recipient or deemed obtained through disclaimers or general terms and conditions. Also, if the consent is obtained through electronic tick-boxes, the consent box shall not be presented as pre-checked.

Secondly, electronic commercial message must contain the following information: the sender's trade name, central registration system number in the title or content of the message, at least one contact detail and an easy way for the recipient to opt out. Recipients may refuse at any time to receive further electronic commercial messages without having to give a reason.

Lastly, service providers and intermediary service providers must keep records of consent for one year after consent is terminated and records of message delivery for one year after the message is delivered.

**Sector-specific legislation**

Although the DP Law is the main data protection instrument, there is sector-specific legislation that governs the protection of personal data under their respective sectors and areas such as the Regulation on Processing of Personal Data and Protection of Privacy in the Electronic Communication Sector,14 Article 73 of the Banking Law15 about banking secrecy and ‘customer secrets’, and the Regulation on Processing of Health Data and Ensuring its Privacy.16

**ix Technological innovation**

**Use of cookies and similar technologies**

Cookies and similar online tracking technologies are not regulated under a specific law; therefore, general rules under the DP Law apply. Processing of personal data for the purposes of targeted and behavioural advertising or profiling, generally, can only be carried out with the explicit consent of the data subject. Consequently, Turkish online media organisations are continuously switching to opt-in schemes for their tracking activities and adding cookie banners to their websites.

**Facial recognition and biometric data**

Biometric data (e.g., fingerprints, facial scans, palm vein data) is categorised as a special category of personal data under the DP Law and can only be processed with the explicit consent of the data subject, unless it is expressly allowed by law. In addition, the use of biometric data is considered to be problematic from a constitutional rights perspective. In a recent decision issued by the Council of State,17 use of facial recognition technologies for shift tracking in a public workplace has been found unconstitutional. In its ruling, the Council stated that use of such technologies even under public settings do fall under the scope of ‘the right to private life’ and that the use of the technology in employee tracking was not envisioned by law.

---

14 Published in the Official Gazette No. 28363 and dated 24 July 2012.
15 Published in the Official Gazette No. 25983 and dated 1 November 2005.
16 Published in the Official Gazette No. 29863 and dated 20 October 2016.
Right of erasure or right to be forgotten

The ‘right to be forgotten’ is not explicitly recognised as a right under the Turkish Constitution. However, recent case law of both Turkish Court of Cassation\(^{18}\) and Supreme Court\(^{19}\) have ruled that the individuals have a ‘right to be forgotten’ under ‘the right to protection of honour and reputation’ and ‘the right to protection of personal data’. In both decisions, the courts made a reference to the ground-breaking \textit{Google Spain} judgment of the ECHR. Consequently, it can be said that a right to be forgotten is emerging by way of case law in Turkey. Moreover, the DP Law recognises that individuals have the right to request deletion or destruction of their personal data under Article 11. Thus, data subjects may request their data to be deleted if the reasons for processing no longer exist.

IV INTERNATIONAL DATA TRANSFER AND DATA LOCALISATION

International transfer of personal data is regulated under Article 9 of the DP Law. The Article prohibits transfer of personal data without obtaining the explicit consent of the data subject. Nevertheless, the second paragraph of the Article permits the transfer of personal data abroad without the data subject’s explicit consent where the following cumulative conditions are met. If one of the conditions set forth in the second paragraph of Article 5 or third paragraph of Article 6 is present and the foreign country to which the personal data will be transferred has an adequate level of protection. If there is not an adequate level of protection, if the data controllers in Turkey and abroad undertake to provide an adequate level of protection in writing and the Data Protection Board has given its permission.

On 17 May 2018, the Board announced the minimum undertakings that must be given by the data controller residing in Turkey and the data processor or controller to which the personal data will be transferred that is residing in an ‘unsafe country’.\(^{20}\) However, as of July 2018, the Board has not yet published the list of ‘safe countries’.

V COMPANY POLICIES AND PRACTICES

Data processing notifications

Data controllers are required to fulfil their obligation to inform data subjects about the processing operations that they will carry out over their personal data. However, the DP Law or secondary legislation does not force data controllers to use any specific methods when informing the data subjects. Aside from the written notices, data controllers may use videos, infographics or other creative methods for informing data controllers as long as they include the minimum information that must be given to the data subjects to fulfil their obligation to inform.

---

\(^{18}\) Court of Cassation, 19th Criminal Chamber, Decision number 2017/5325 dated 5 June 2017.

\(^{19}\) Supreme Court, application number 2013/5653. Published in the Official Gazette No. 29811 and dated 24 August 2016.

ii Data processing inventory

Data controllers who are obliged to register with the Registry under the Regulation on the Registry of Data Controllers are expected to create a ‘data processing inventory’ and a personal data retention and destruction policy that is compliant with the inventory. The data processing inventory is where data controllers explain and detail their data processing operations in accordance with their business processes. The inventory shall contain the following:

- a purposes for processing personal data;
- b data categories;
- c recipient groups to which data is transferred;
- d subject groups of the data;
- e maximum retention period required by the processing purpose;
- f personal data to be transferred abroad; and
- g measures taken regarding data security.

Furthermore, the data processing inventory shall be the basis for the notifications to be made to the Registry, and Article 5 of the Communiqué on the obligation to inform states that the information provided during the fulfilment of the obligation to inform must be compliant with the information disclosed to the Registry. Therefore, the information within the inventory is fundamental for lawfully fulfilling the obligation to register with the registry and the obligation to inform the data subjects.

iii Data security practices

With regards to the security obligations, the DP law obliges data controllers to take ‘all technical and organisational measures to ensure adequate level of data security’. Therefore, the type of data security measures to be taken by the data controllers are not determined by law. The Board has published a guidebook on data security to highlight certain measures that can be taken by the data controllers. The measures suggested by the Board include conducting data protection risk analyses, preparing internal data protection policies (incident response plans, data access policies etc.), signing NDAs with employees, using firewalls and conducting penetration tests. Measures included in the guidebook are not mandatory for each and every data controller. Data controllers must decide themselves which measures are adequate for their data processing operations. However, measures included in the guidebook are explanatory on the interpretation on what type of measures the Board expects data controllers to take to ensure ‘adequate data security’.

VI DISCOVERY AND DISCLOSURE

According to Article 332 of the Turkish Criminal Procedure Law, criminal courts and prosecutors may request information, including those containing personal data, during criminal proceedings. Similarly, civil courts may request information that relates to the case at hand from the parties of the case or even third parties. The DP Law expressly states that provisions of the law shall not be applied when personal data is processed by judicial authorities with regards to investigation, prosecution, trial or execution procedures.

In addition to the judicial authorities, a number of onsite auditing rights are granted to multiple public bodies over entities that are active in their respective sectors. To exemplify, by the rights granted in their founding laws, the Energy Market Regulatory Authority, the
Banking Regulation and Supervision Authority, and the Information Technologies and Communication Agency may request information from relevant players of their corresponding sectors and may conduct on-site auditing activities. During the audits, supervisory authorities may access records which include personal data.

Lastly, Turkey is a party to the Convention of 1 March 1954 on civil procedure and multiple bilateral treaties on legal assistance. Therefore, data may be disclosed in response to lawful requests made by foreign governments complying with due process under the Convention.

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

The Board is the main authority with regards to protection of personal data. The Board is established by the DP Law and the law grants extensive investigatory and sanctioning power to the authority. Pursuant to Article 15 of the DP Law, the Board may conduct necessary investigations *ex officio* or upon notification about breaches of the DP Law. Data controllers are obliged to comply with the information requests made by the Board and allow them to conduct onsite audits. If a breach is found, the Board notifies the relevant data controller to correct the unlawful situation. The data controller must comply with the notification without delay and within 30 days of the notification at the latest.

Article 18 of the DP Law lists several misdemeanours concerning data protection and the range of the administrative fines tied to them. Breach of the obligation to inform or to ensure the security of personal data, and failure to fulfil the obligation to register with the data controller registry or to comply with the decision given by the Board are considered misdemeanours and are subject to separate administrative fines ranging from 5,000 to 1 million Turkish lira.

During its investigations, if the Board finds out that a particular breach is widespread, it may issue a principle decision and publish it. It is mandatory for data controllers to comply with principle decisions. The Board has published three principle decisions to date about phonebook applications, the implementation of privacy measures on counters and booths, and data breaches caused by data controllers’ personnel. In addition to the principle decisions, the Board is periodically publishing guidelines and videos and arranges seminars to inform the public and data controllers about data protection issues.

In addition to the mentioned administrative sanctions, Turkish Criminal Code lists certain crimes that are related to unlawful processing of personal data. For example, unlawful recording, distribution or obtaining of personal data are crimes that are punished by imprisonment of the perpetrator between one to four years.

ii Recent enforcement cases

The Board have recently published summaries of eight of its enforcement decisions on its website. Although the summaries did not include the identities of the data controllers or the amount of fines, the reasons given by the Board were enlightening. The majority of fines were sanctioned owing to a breach of data security obligations, even when the breach was caused

---

because of a breach of data processing principles. For example, the Board sanctioned a bank because it violated the principle of ‘data minimisation’ when it provided a six-month account statement of its customer to a civil court when the court only asked for the statement of the last three months. In another example, the Board found a breach of data security obligations where the data controller had made the explicit consent of the data subject a precondition for the provision of certain goods or services.

iii  **Private litigation**

Under Article 11 of the DP Law, data subjects have the right to request compensation for the damages if they incur any losses due to unlawful processing of personal data. Accordingly, data subjects may request for pecuniary or non-pecuniary damages from the data controllers in case of unlawful processing of personal data.

**VIII  **CONSIDERATIONS FOR FOREIGN ORGANISATIONS**

The DP Law applies to domestic and foreign data controllers alike. Although the DP Law does not provide a territorial scope for its application, it is generally regarded as applicable if the processing takes place within the borders of Turkey. Consequently, foreign data controllers are expected to comply with obligations listed within the DP Law and its secondary legislation if they process non-Turkish citizens’ data outside of Turkey.

The notable obligations that are required from foreign data controllers are to register with the data controller registry and to assign a ‘data controller representative’. According to Article 11 of the Regulation on Data Controller Registry, data controllers who are not resident in Turkey are expected to appoint a data controller representative who will carry out communications by data subjects and the Board with the foreign data controller.

One misconception that is common in practice is mistaking the data controller representative with the data protection officer (DPO) regulated under the GDPR. There is no obligation to appoint a DPO under the DP Law. Additionally, data controller representatives are positioned more as a contact point and they do not have extensive data-protection-related responsibilities as significant as those a DPO would hold under the GDPR.

The data controller representative must represent its associated data controller on at least the following issues (though the list can be expanded in the appointment decision):

1. accepting the notifications or correspondence made by the Board on behalf of the data controller and responding to the requests directed to the data controller in the name of the data controller; and
2. collecting and forwarding the data subject applications to the data controller;
3. transmitting the responses given by data controllers in relation to data subject applications; and
4. carrying out actions and operations related to the Registry on behalf of the data controller.

**IX  **CYBERSECURITY AND DATA BREACHES**

i  **Cybersecurity**

There is no catch-all cybersecurity legislation that is applicable to every entity. There are multiple sector-specific regulations that require organisations from critical sectors to employ cybersecurity measures to safeguard their information systems. For example, their
sector-specific legislation requires organisations related to capital markets (including on-stock companies)\textsuperscript{22} and entities from sectors such as insurance,\textsuperscript{23} banking\textsuperscript{24} and payment services\textsuperscript{25} to employ certain measures related to cybersecurity.

On the state level, the National Computer Emergency Response Center (CERT) has been established within the Information and Communication Technologies Authority.\textsuperscript{26} Missions of the CERT include thwarting cybersecurity risks in Turkey, taking measures to minimise the impact of cyberattacks, and sharing information about cybersecurity with public and private entities.

ii Data breaches

The most important data breach notification obligation under Turkish law is the personal data breach notification stipulated under the DP Law. Data controllers are required to notify the data subject and the Board ‘in case personal data is acquired by others through unlawful means’. Data breaches that fall under this notification obligation are not categorised by their scope, seriousness or its possible adverse effects. Thus, all data breaches where personal data is obtained unlawfully by third parties must be notified to the data subject and the Board. The relevant provision of the Law states that the notification should be made ‘as soon as possible’. However, the Law does not state a specific maximum period for notification and the Board has not yet issued such an opinion. Lastly, the Board has not yet issued any formal or content requirements with regards to the notification obligation.

X OUTLOOK

Data protection is a relatively new regulatory area for Turkey. Yet the developments that we have observed in the area in the last two years have been fast and are not expected to slow down in the following years. For the near term, two of the most significant developments that are expected are the activation of the data controller registry and the publishing of the list of countries that have an ‘adequate level of personal data protection’ by the Board. It is advisable for the foreign entities to be on the watch for these two legal developments as these will have significant effects for their businesses in Turkey.

The GDPR has had an impact on the Turkish entities owing to its extended territorial scope and high level of monetary fines. Turkish businesses that are active in the European market are mindful of the requirements brought by it. The DP Law was prepared by taking note of the EU Data Protection Directive of 1995 and it is known that the Board is paying close attention to the data protection developments in Europe. If the ‘Europeanisation’ trend continues for data protection in Turkey, in the long term amendments to the DP Law that are in line with the provisions of the GDPR should not come as a surprise.

\textsuperscript{23} See Regulation on Supervision and Auditing of Insurance and Individual Annuity Insurance Sectors, published in the Official Gazette No. 28054 and dated 14 September 2011.
\textsuperscript{25} See Regulation on the Activities of the Payment and Security Settlement Systems, published in the Official Gazette No. 29044 and dated 28 June 2014.
\textsuperscript{26} CERT Website available in English: https://www.usom.gov.tr/.
I OVERVIEW

Like other countries in Europe, the United Kingdom has passed legislation designed to supplement the data protection requirements of the EU General Data Protection Regulation (GDPR), which came into force on 25 May 2018, repealing the EU Data Protection Directive 95/46/EC (the Data Protection Directive) and which regulates the collection and processing of personal data across all sectors of the economy. The UK Data Protection Act 2018 (DPA 2018), which came into force on 23 May 2018, repeals the UK Data Protection Act 1998 (DPA 1998), introduces certain specific derogations that further specify the application of the GDPR in UK law, in addition to transposing the data protection and national security provisions of the EU Law Enforcement Directive 2016/680 as well as granting powers and imposing duties on the national data supervisory authority, the UK’s Information Commissioner’s Office (ICO).

II THE YEAR IN REVIEW

In preparation for the coming into force of the GDPR, the ICO has published an extensive guide on the GDPR that explains how the substantive data protection provisions of the GDPR should be complied with when processing personal data. The guide also refers to the DPA 2018 where relevant and also contains links to other relevant ICO guidance. The ICO has also published detailed guidance on consent as a lawful basis for processing. Its guide on the DPA 2018, published when it was a bill going through Parliament, is currently being updated to reflect the finalised text of the DPA 2018. The ICO has also published a Guide to

---

1 William RM Long is a partner, Géraldine Scali is a counsel and Francesca Blythe is an associate at Sidley Austin LLP.
4 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/JHA.
Law Enforcement processing, highlighting the key requirements of Part 3 of the DPA 2018 that controllers and processors have to comply with when processing personal data for ‘law enforcement purposes’.

In April 2018, the Information Commissioner, Elizabeth Denham, stated the ICO is preparing for the post-Brexit environment, ‘in order to ensure that the information rights of UK citizens are not adversely affected’ by Brexit.6 It is clear that the UK leaving the EU on 29 March 2019 will be highly significant from a data protection perspective and further details are provided in Section XII below.

III REGULATORY FRAMEWORK

i Privacy and data protection laws and regulations

Until 23 May 2018, data protection in the United Kingdom was mainly governed by the DPA 1998, which implemented the Data Protection Directive into national law and entered into force on 1 March 2000. Data protection in the UK is now governed by the DPA 2018, which replaced the DPA 1998 on 23 May 2018. The DPA 2018 is split into six main parts; general processing, law enforcement processing, intelligence services processing, the UK data supervisory authority, the Information Commissioners Office (ICO), enforcement, and supplementary and final provisions. This chapter will focus on the general processing sections of the DPA 2018.

The Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended by the Privacy and Electronic Communications (EC Directive) (Amendments) Regulations 2011) (PECR) regulate direct marketing, but also the processing of location and traffic data and the use of cookies and similar technologies. The PECR implemented Directive 2002/58/EC7 (as amended by Directive 2009/136/EC) (the ePrivacy Directive). The ICO has also updated its guide to PECR to take into account the GDPR.

On 10 January 2017, the European Commission issued a draft of the proposed Regulation on Privacy and Electronic Communications (the ePrivacy Regulation) to replace the existing ePrivacy Directive.8 The European Commission’s original timetable for the ePrivacy Regulation was for it to apply in EU law and have direct effect in Member State law from 25 May 2018, coinciding with the GDPR’s entry into force. However, owing to ongoing trilogue negotiations between the Commission, the European Parliament and the European Council to agree on a finalised text, the ePrivacy Regulation is not now expected to come into force until sometime in 2019 at the earliest. The ePrivacy Regulation, which will complement the GDPR, will have direct effect in Member States including the United Kingdom if it enters into force before 29 March 2019, the United Kingdom’s scheduled departure date from the European Union, and provides additional sector-specific rules including in relation to marketing and the use of website cookies.

The key changes in the proposed ePrivacy Regulation will:

a require a clear affirmative action to consent to cookies;

---


© 2018 Law Business Research Ltd
b attempt to encourage the shifting of the burden of obtaining consent for the use of cookies to website browsers; and

c make consent for direct marketing harder to obtain and require it to meet the standard set out in the GDPR; however, existing exceptions (such as the exemption that applies where there is an existing relationship and similar products and services are being marketed) are likely to be retained.

Key terms under the DPA 2018

Under the DPA 2018, the terms used in the DPA 2018 have the same meaning as they have in the GDPR. The key terms are:

a data controller: a natural or legal person who (either alone, or jointly with others) determines the purposes and means of the processing of personal data;

b data processor: a natural or legal person who processes personal data on behalf of the data controller;

c data subject: an identified or identifiable individual who is the subject of personal data;

d personal data: any information relating to a identified or identifiable individual 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, psychological, genetic, mental, economic, cultural or social identity of that individual;

e processing: any operation or set of operations that are 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; and

f special categories of data: personal data revealing the racial or ethnic origin of the data subject, his or her political opinions, his or her religious or philosophical beliefs, whether the data subject is a member of a trade union, genetic data, biometric data for the purpose of uniquely identifying the data subject, data concerning the data subject’s health or data concerning the data subject’s sexual life or sexual orientation.

Data protection authority

The DPA 2018 and the PECR are enforced by the ICO and from 25 May 2018, the ICO has powers of enforcement in relation to organisations complying with the data protection requirements in the GDPR. Once the ePrivacy Regulation is finalised and takes effect, the ICO will also enforce the ePrivacy Regulation (assuming the ePrivacy Regulation takes effect in the UK). The ICO also enforces and oversees the Freedom of Information Act 2000, which provides public access to information held by public authorities.

The ICO has independent status and is responsible for:

a maintaining the public register of data controllers;

b promoting good practice by giving advice and guidance on data protection and working with organisations to improve the way they process data through audits, arranging advisory visits and data protection workshops;

9 Section 5 of the DPA 2018.
c ruling on complaints; and

d taking regulatory actions.

IV GENERAL OBLIGATIONS FOR DATA HANDLERS

The DPA 2018 does not create additional principles and obligations in relation to general processing of personal data under the GDPR. Therefore, data controllers must comply with the GDPR’s data protection principles and ensuing obligations when established in the UK or processing personal data of UK data subjects.

i First data protection principle: fair, lawful and transparent processing

Personal data must be processed fairly, lawfully and in a transparent manner in relation to the data subject. This essentially means that the data controller must:

a have a legitimate ground for processing the personal data;

b not use personal data in ways that have an unjustified adverse effect on the data subject concerned;

c be transparent about how the data controller intends to use the personal data, and give the data subject appropriate privacy notices when collecting their personal data;

d handle a data subject’s personal data only in ways they would reasonably expect and consistent with the purposes identified to the data subject; and

e make sure that nothing unlawful is done with the personal data.

The UK DPA 2018 does not introduce any further requirements in relation to the first data protection principle.

ii Legal basis to process personal data

As part of fair and lawful processing, processing of personal data must be justified by at least one of six specified grounds in Article 6 of the GDPR:

a the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

b 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;

c processing is necessary for compliance with a legal obligation to which the controller is subject;

d processing is necessary in order to protect the vital interests of the data subject or of another individual;

e 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; and

f 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.
The ICO guide on the GDPR contains guidance on the reliance of each Article 6 legal basis. In particular, the ICO has also published detailed guidance on legitimate interests together with a legitimate interest assessment template that covers three tests controllers should conduct as part of any assessment:

a) the purpose test – to assess whether there is a legitimate interest behind the processing;

b) the necessity test – to assess whether the processing is necessary for the purpose it has identified; and

c) the balancing test – to consider the impact on data subjects’ interests and rights and freedoms and to assess whether they override the controller’s own legitimate interests.

Additionally, the ICO’s guidance on the GDPR, contains a section on consent, which makes reference to the GDPR’s high standard on consent, being unambiguous, involving a clear affirmative action and requiring distinct or granular options to give consent for distinct processing operations. As consent must be freely given, certain organisations in a position of power over their data subjects may find it difficult to show valid freely given consent, for example, consent obtained from employees by their employers is unlikely to be freely given as such consent is not considered freely given or a genuine choice, with employees possibly facing employment consequences as a result of failing to provide consent.

The GDPR and DPA 2018 apply a stricter regime for special categories of personal data and criminal convictions data, where such data may only be processed on the basis of certain limited grounds which constitute fair and lawful processing, including, for example, where the controller had obtained explicit consent of the data subject or where necessary for the purposes of carrying out its obligations and exercising specific rights in the field of employment and social security.

iii Special categories of personal data

The GDPR distinguishes between personal data and special categories of personal data (or sensitive data). In order to lawfully process sensitive personal data, controllers must identify a legal ground under Article 6 of the GDPR and a condition under Article 9 of the GDPR. The DPA 2018 introduces additional conditions for processing sensitive personal data. Part 1 of Schedule 1 of the DPA 2018 includes the following conditions in relation to employment, health and research:

a) employment, social security and social protection;

b) health or social care purposes;

c) public health; and

d) research etc.

Part 2 of Schedule 1 of the DPA 2018 includes 23 conditions in relation to processing necessary for reasons of substantial public interest including, for example:

a) equality of opportunity or treatment;

b) racial and ethnic diversity at senior levels of organisation;

c) regulatory requirements relating to unlawful acts and dishonesty etc.;

---

11 ICO, Sample LIA template.
12 Articles 9 and 10 of the GDPR, Sections 10 and 11 and Schedule 1 of the DPA 2018.


Where processing personal data in reliance on a condition under the DPA 2018 the controller will need to have in place an ‘appropriate policy document’ which explains the controller’s procedures for securing compliance with the principles in Article 5 of the GDPR, and explains the controller’s policies as regards the retention and erasure of personal data processed in reliance on the DPA 2018 condition.

iv Criminal records personal data

Criminal records and offences data are not included within the scope of special categories of personal data. Section 11 of the DPA 2018 states that references in the GDPR to criminal records and offences data include personal data relating to the alleged commission of offences by the individual, or proceedings for an offence committed or alleged to have been committed by the individual.

In order to lawfully process criminal records and offences data, controllers must: (1) identify a legal ground under Article 6 of the GDPR; and (2) carry out the processing under the control of official authority or when the processing is authorised by Union or Member State law. Where the processing of criminal records and offences data is not carried out under the control of official authority, such processing is authorised by UK law for purposes of Article 10 only if the processing meets a condition in Parts 1, 2 or 3 of Schedule 1 of the DPA 2018.

Part 3 of Schedule 1 of the DPA 2018 sets out a number of conditions for the processing of criminal records and offences data including those that relate to:

- consent;
- protecting data subjects vital interests;
- processing by not-for-profit bodies;
- personal data in the public domain;
- legal claims;
- judicial acts;
- administration of accounts used in commission of indecency offences involving children; and
- extension of the insurance conditions in Part 2 of Schedule 1.

Part 3 also permits a controller to rely on a Part 2 condition and the requirement that the processing be in the substantial public interest can be disapplied. Where processing criminal records and offences data in reliance on a condition under the DPA 2018 the controller will need to have in place an ‘appropriate policy document’.

v Health Data

Data concerning health falls within scope of the special categories of personal data under Article 9 of the GDPR. The GDPR defines ‘data concerning health’ as ‘personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status’.

One of the lawful processing grounds for health data is Article 9(2)(j) of the GDPR where processing is necessary for scientific research purposes. To rely on this legal ground the
processing must comply with Article 89(1) of the GDPR which requires that the processing be subject to appropriate safeguards which ensure technical and organisational measures are in place in particular, to comply with the principle of data minimisation.

Article 19 of the DPA 2018 states that the processing will not meet these requirements where:

- it is likely to cause substantial damage or distress to an individual; or
- the processing is carried out to support measures or decisions relating to a particular individual, unless this includes purposes of approved medical research.

The DPA 2018 includes exemptions from the data subject rights for data concerning health where:

- it is processed by a court, supplied in a report or other evidence given to a court, and under specified rules (i.e., those relating to family and children’s hearings in the courts) may be withheld from an individual;¹³
- the request is made by someone with parental responsibility for a person under the age of 18 (or 16 in Scotland) and the data subject has an expectation that the information would not be disclosed to the requestor or has expressly indicated should not be disclosed.¹⁴

The DPA 2018 also includes an exemption from the subject access right to health data where disclosure would likely cause serious harm to the physical or mental health of the individual or another person.¹⁵

vi Data protection officer

The appointment of a data protection officer (DPO) in the private sector is required where an organisation’s core activities (i.e., the primary business activities of an organisation), involve¹⁶:

- the regular and systematic monitoring of individuals on a large scale – for example, where a large retail website uses algorithms to monitor the searches and purchases of its users and, based on this information, it offers recommendations to them; or
- the large-scale processing of special categories of personal data (e.g., health data) or personal data relating to criminal convictions and offences – for example, a health insurance company processing a wide range of personal data about a large number of individuals, including medical conditions and other health information.

The ICO states in its guidance on the appointment of DPOs, that regardless of whether the GDPR requires an organisation to appoint a DPO, the organisation must ensure that it has sufficient staff and resources to discharge its obligations under the GDPR and that a DPO can be seen to play a key role in an organisation’s data protection governance structure and to help improve accountability. The guidance further advises that should an organisation decide that it does not need to appoint a DPO it is recommended that this decision be recorded to help demonstrate compliance with the accountability principle.

¹³ Section 3, Part 2 of Schedule 3 to the DPA.
¹⁴ Section 4, Part 2 of Schedule 3 to the DPA.
¹⁵ Section 2(2), Part 2 of Schedule 3 to the DPA.
¹⁶ Section 37(1)(b) and (c) of the GDPR.
The DPO must be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices.\textsuperscript{17} The data controllers and data processors who do not meet the criteria for a required appointment of a DPO may voluntarily appoint one and are required to notify the ICO of any voluntary appointment.

Required and voluntary appointments of DPOs must be notified to the ICO in the form of an email, including:

- the contact details of the DPO;
- the registration number of the data controller or processor; and
- whether the appointment of the DPO was required or voluntary.

The ICO will publish the name of the DPO on the Data Protection Public Register, where the data controller or data processor has consented to publication.

Section 71 of the DPA 2018 requires controllers to entrust their DPO with the following non-exhaustive tasks:

- informing and advising the controller, any processor engaged by the controller, and any employee of the controller who carries out the processing of personal data, of that person’s obligations under the DPA 2018;
- providing advice on the carrying out of a data protection impact assessment (see below) and monitoring compliance;
- cooperating with the ICO;
- acting as the contact point for the ICO on issues relating to processing of personal data;
- monitoring compliance with the policies of the controller in relation to the protection of personal data; and
- monitoring compliance by the controller of Section 71 of the DPA 2018.

vii Registration with the ICO

Under the UK Data Protection (Charges and Information) Regulations 2018\textsuperscript{18} (the Charges and Information Regulations), controllers are required to register with the ICO and pay a charge fee to the ICO. The cost of the charge fee depends on the number of employees and the turnover of the organisation. The Charges and Information Regulations have established three tiers of fees ranging from £40 to £2,900. Registering with the ICO consists of filling in an online form on the ICO website and making the payment of a fee online, which must be paid when the controller registers for the first time and then every year when the registration is renewed.

Also Article 30 of the GDPR requires controllers to keep a record of their processing activities. Data processors are also under an obligation to keep a record of processing activities carried out on behalf of data controllers. The ICO has published template controller and processor records of processing activities. Such records will have to be provided to the ICO upon request.\textsuperscript{19}

\textsuperscript{17} Article 37(5) of the GDPR.

\textsuperscript{18} Data Protection (Charges and Information) Regulations 2018/480.

\textsuperscript{19} Article 30 of the GDPR.
viii  Information notices

Controllers must provide data subjects with information on how their personal data is being processed pursuant to Articles 13 and 14 of the GDPR. The list of information to be provided varies if the personal data has been obtained directly from the data subject or from a third party. The DPA 2018 introduces no further requirements in relation to the notices given to data subjects.

The ICO, in its guidance on the GDPR,\(^\text{20}\) in particular on the data subject’s right to be informed, suggests the information notice can take many forms, including:

\textit{a} a layered approach: this will usually be a short notice containing key privacy information, with additional layers of more detailed information;

\textit{b} dashboards: preference management tools that inform people how the controller will use their personal data and provides the option for data subjects to manage what happens with the processing of their personal data;

\textit{c} just-in-time notices: relevant and focused privacy notices delivered at the time the personal data is collected;

\textit{d} icons: small, meaningful symbols that highlight the existence of data processing; and

\textit{e} mobile and smart device functionalities: these include pop-ups, voice alerts and mobile device gestures.

ix  Data protection impact assessments

Controllers are under an obligation to carry out a DPIA where the processing is likely to result in a high risk to individuals. While the GDPR provides three specific examples of where a DPIA should be carried out, the ICO in its guidance on DPIAs states that it is also good practice to do a DPIA for any other major project that requires the processing of personal data. The ICO has also published a DPIA Screening Checklist that sets out:

\textit{a} instances where a DPIA should always be carried out (e.g., where processing special categories of personal data or criminal offence data on a large scale, or where processing personal data without providing a privacy notice directly to the individual); and

\textit{b} instances where a DPIA should be considered (e.g., where processing on a large scale, or where using innovative technological or organisational solutions).

Section 64 of the DPA 2018 requires controllers to include in their DPIA:

\textit{a} a general description of the envisaged processing operations;

\textit{b} an assessment of the risks to the rights and freedoms of data subjects;

\textit{c} the measures envisaged to address those risks; and

\textit{d} safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with Section 64 of the DPA 2018, taking into account the rights and legitimate interests of the data subjects and other persons concerned.

The ICO guidance also recommends that where a controller decides not to carry out a DPIA, the reasons for this decision are documented.\(^\text{21}\)


Second data protection principle: processing for specified, explicit and lawful purposes (purpose limitation)

Personal data can only be obtained for specified, explicit and lawful purposes, and must not be further processed in a manner that is incompatible with those purposes.

The UK DPA 2018 does not introduce any further requirements in relation to the second data protection principle.

The ICO’s published guidance on GDPR includes a section on purpose limitation, where it requires controllers to specify the purposes of the processing to data subjects at the outset of the processing, in the form of records of the processing activities that controllers are required to maintain and information notices that are required to be given to data subjects prior to the processing.

Third data protection principle: personal data must be adequate, relevant and limited to what is strictly necessary (data minimisation)

A controller must ensure that the personal data it holds is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

The UK DPA 2018 does not introduce any further requirements in relation to the third data protection principle.

The ICO’s published guidance on the GDPR, contains guidance on data minimisation, requiring controllers to identify the minimum amount of personal data needed to fulfil its processing purposes, noting if the processing carried out does not help the controller to achieve its purposes the personal data held is most likely inadequate.

The ICO recommends controllers should carry out periodic reviews of their processing in order to check that the personal data held is still relevant and adequate for its purposes, deleting any personal data that is no longer needed.

Fourth data protection principle: personal data must be accurate and where necessary kept up to date (accuracy)

Controllers must ensure that personal data is accurate and, where necessary, kept up to date. The ICO recommends controllers take reasonable steps to ensure the accuracy of any personal data obtained, ensure that the source and status of any personal data is clear, and carefully consider any challenges to the accuracy of information and whether it is necessary to periodically update the information.

© 2018 Law Business Research Ltd
United Kingdom

xiii Fifth data protection principle: personal data must be kept in a form that permits the identification of data subjects for no longer than is necessary (storage limitation)

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. In practice, this means that the controller must review the length of time it keeps personal data and consider the purpose or purposes it holds the information for in deciding whether (and for how long) to retain this information. Controllers must also securely delete personal data that is no longer needed for this purpose or these purposes, and update, archive or securely delete information if it goes out of date.

It is good practice to establish standard retention periods for different categories of information (e.g., employee data and customer data). To determine the retention period for each category of information, controllers should take into account and consider any legal or regulatory requirements or professional rules that would apply.26

The ICO, in its published guidance on the GDPR, contains guidance on storage limitation, recommending ensuring that controllers erase or anonymise personal data27 where controllers no longer need it, in order to reduce the risk of the personal data becoming excessive, irrelevant, inaccurate or out of date. This will also help controllers comply with the data minimisation and accuracy principles, while ensuring the risk that the controller uses the personal data in error is reduced.

The ICO also recommends in its GDPR storage limitation guidance28 that it is good practice for controllers to adopt clear policies on retention periods and erasure, which can help reduce the burden of dealing with questions from data subjects about retention and access requests for the erasure of personal data.

xiv Sixth data protection principle: personal data must be processed in a manner that ensures appropriate security of personal data

Personal data must be processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. Where a controller uses a data processor to process personal data on its behalf, the controller must ensure that it has entered into a written contract that obliges the data processor to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of processing personal data.

The ICO recommends, in its published guidance on security under the GDPR,29 before deciding what measures are appropriate, controllers should assess the personal data risk by carrying out an information risk assessment. A controller should review the personal data

28 ibid.
it holds, and the way it is used to assess how valuable, sensitive or confidential the personal
data is, including assessing any potential damage or distress that may be caused if the data is
compromised.

When carrying out the assessment, the ICO recommends taking into account:

a. the nature and extent of the controller’s premises and computer systems;
b. the number of staff the controller has;
c. the extent of the staff’s access to the personal data; and

d. any personal data held or used by the processor acting on the controller’s behalf.30

In addition, the ICO recommends that controllers should aim to build a culture of security
awareness within the organisation, identifying a person with day-to-day responsibility for
information security within the organisation and ensuring the person has the appropriate
resources and authority to do their job effectively.31

The ICO considers encryption to be an appropriate technical measure owing to its
widespread availability and relatively low cost of implementation.32 However, there are other
measures, such as pseudonymisation of data and anonymisation that can also be used to
ensure the security of personal data.

The technical and organisational measures controllers have in place are also considered
by the ICO when deciding whether to impose an administrative fine on the controller for the
infringement of the GDPR and DPA 2018.

xv  Seventh data protection principle: Integrity and Confidentiality

Under the GDPR, personal data must be processed in a manner that ensures appropriate
security of personal data.

The DPA 2018 introduces no further derogations to this principle.

xvi  Eighth data protection principle: Accountability

The data protection principle of accountability under Article 5.2 of the GDPR is prevalent
through the GDPR and requires controllers to not only comply with the GDPR but to
demonstrate its compliance with the data protection principles under GDPR.

In addition to putting in place appropriate technical and organisational measures, the
ICO suggest in their GDPR accountability guidance33 a number of measures controllers can
adopt to comply with the accountability principle, including:

a. adapting and implementing data protection policies;
b. taking a ‘data protection by design and default’ approach;
c. when engaging with vendors processing personal data of individuals in the EU, have
   written contracts in place that comply with Article 28 of the GDPR;

d. maintain records of its processing activities;
e. record and, where necessary, report personal data breaches;

30 ibid.
31 ibid.
32 ibid.
33 ICO, Guide to the General Data Protection Regulation (GDPR)/Accountability and governance, accessible
The ICO notes that if controllers adopt a privacy management framework this can help embed accountability measures and create a culture of privacy across the controller’s organisation. The framework could include:

1. robust programme controls informed by the GDPR requirements;
2. appropriate reporting structures; and
3. assessment and evaluation procedures.

V TECHNOCICAL INNOVATION AND PRIVACY LAW

1. **Anonymisation**

Neither the DPA 2018 nor the GDPR apply to anonymous data. However, there has been a lot of discussion in the past over when data is anonymous and the methods that could be applied to anonymise data.

When the DPA 1998 was in force, the ICO published guidance on anonymisation that recommended organisations using anonymisation have in place an effective and comprehensive governance structure that should include:

1. a senior information risk owner with the technical and legal understanding to manage the process;
2. staff trained to have a clear understanding of anonymisation techniques, the risks involved and the means to mitigate them;
3. procedures for identifying cases where anonymisation may be problematic or difficult to achieve in practice;
4. knowledge management regarding any new guidance or case law that clarifies the legal framework surrounding anonymisation;
5. a joint approach with other organisations in the same sector or those doing similar work;
6. use of a privacy impact assessment;
7. clear information on the organisation’s approach to anonymisation, including how personal data is anonymised and the purpose of the anonymisation, the techniques used and whether the individual has a choice over the anonymisation of his or her personal data;
8. a review of the consequences of the anonymisation programme; and
9. a disaster-recovery procedure should re-identification take place and the individual’s privacy be compromised.

The guidance has not yet been updated to take into account the entry into force of the GDPR and DPA 2018.
ii  **Big data**

The DPA 2018 does not prohibit the use of big data and analytics. The ICO issued guidance in July 2014 and revised it in August 2017\[36\] considering data protection issues raised by big data. The ICO suggested how data controllers can comply with the DPA 2018 and the GDPR while using big data, covering a broad range of topics including anonymisation, privacy impact assessments, repurposing data, data minimisation, transparency and subject access. The guidance included three questions on which the ICO invited feedback. A summary of feedback on big data and data protection and the ICO position was published in April 2015.\[37\]

In addition, the Financial Conduct Authority (FCA) published in March 2017 a feedback statement following its call for input on big data on retail general insurance.\[38\] The FCA’s key findings were that although big data is producing a range of benefits for consumers in motor and home insurance, there are also concerns about its impact on data protection. To address some of these concerns the FCA proposed to co-host a roundtable with the ICO and various stakeholders to discuss data protection and the use of personal data in retail general insurance.

iii  **Bring your own device**

The ICO has published guidance for companies on implementing bring your own device (BYOD)\[39\] programmes allowing employees to connect their own devices to company IT systems. Organisations using BYOD should have a clear BYOD policy so that employees connecting their devices to the company IT systems clearly understand their responsibilities.

To address the data protection and security breach risks linked to BYOD, the ICO recommends that companies take various measures, including:

- **a** considering which type of corporate data can be processed on personal devices;
- **b** how to encrypt and secure access to the corporate data;
- **c** how the corporate data should be stored on the personal devices;
- **d** how and when the corporate data should be deleted from the personal devices; and
- **e** how the data should be transferred from the personal device to the company servers.

Organisations should also install antivirus software on personal devices, provide technical support to the employees on their personal devices when they are used for business purposes, and have in place a ‘BYOD acceptable-use policy’ providing guidance to users on how they can use their own devices to process corporate data and personal data.

The guidance has not yet been updated to take into account the entry into force of the GDPR and DPA 2018.

---


\[37\] ICO, Summary of Feedback on Big Data and Data Protection and ICO Response, 10 April 2015.

\[38\] FCA, FS16/5, Call for Inputs on Big Data in retail general insurance.

\[39\] ICO, Guidelines on Bring Your Own Device (BYOD), 2013.
iv Cloud computing

The use of cloud computing and how it complies with EU data protection requirements has been a subject of much discussion recently. The ICO, like many other data protection authorities in the EU, published guidance on cloud computing, in 2012.\(^{40}\)

The ICO proposes a checklist that organisations can follow prior to entering into an agreement with a cloud provider, with questions on confidentiality, integrity, availability, and other legal and data protection issues.\(^{41}\)

According to the guidance, cloud customers should choose their cloud provider based on economic, legal and technical considerations. The ICO considers it is important that, at the very least, such contracts should allow cloud customers to retain sufficient control over the data to fulfil their data protection obligations.

The ICO is currently updating the cloud computing guidance to reflect the entry into force of the GDPR and DPA 2018.

v Cookies and similar technologies

In 2009, the e-Privacy Directive 2002/58/EC was amended.\(^{42}\) This included a change to Article 5(3) of the e-Privacy Directive requiring consent for the use of cookies and similar technologies. This new requirement was implemented in the United Kingdom through the PECR. As a result, organisations now have an obligation to obtain consent of website users to place cookies or similar technologies on their computers and mobile devices.\(^{43}\) The consent obligation does not apply where the cookie is used ‘for the sole purpose of carrying out the transmission of a communication over an electronic communication network’ or is ‘strictly necessary’ to provide the service explicitly requested by the user. This exemption is applied restrictively and so could not be used when using analytical cookies. Organisations must also provide users with clear and comprehensive information about the purposes for which the information, such as that collected through cookies, is used.

The ICO has published guidance on the use of cookies, and provides recommendations on how to comply with the PECR requirements and how to obtain consent. Its PECR guidance, in particular its section on cookies, has been updated in light of the entry into force of the GDPR, where it notes that consent does not necessarily have to be ‘explicit’, however it must be a clear positive action to constitute valid consent.\(^{44}\)

The ePrivacy Regulation will complement the GDPR and provide additional sector-specific rules, including in relation to the use of website cookies.\(^{45}\)

---

\(^{41}\) See the European Union Overview chapter for more details on cloud computing.
\(^{42}\) Directive 2009/136/EC.
\(^{43}\) PECR Regulation 6.
\(^{45}\) See the European Union Overview chapter for more details on the proposed ePrivacy Regulation.
VI SPECIFIC REGULATORY AREAS

i Employee data

There is no specific law regulating the processing of employee data. However, the ICO has published an employment practices code and supplementary guidance to help organisations comply with the DPA and to adopt good practices.46

The code contains four parts covering:

a recruitment and selection, providing recommendations with regard to the recruitment process and pre-employment vetting;
b employment records, which is about collecting, storing, disclosing and deleting employees’ records;
c monitoring at work, which covers employers’ monitoring of employees’ use of telephones, internet, email systems and vehicles; and
d workers’ health, covering occupational health, medical testing and drug screening.

The code and supplementary guidance has not yet been updated to reflect the entry into force of the GDPR and DPA 2018.

ii Employee monitoring47

The DPA 2018 does not prevent employers from monitoring their employees. However, monitoring employees will usually be intrusive, and workers have legitimate expectations that they can keep their personal lives private. Workers are also entitled to a degree of privacy in their work environment.

DPIAs must be carried out when the processing of personal data is likely to result in a high risk to the rights and freedoms of individuals. The Article 29 Working Party Guidance on Data Protection Impact Assessments48 provides examples of when a DPIA should be carried out. An employee monitoring programme is identified by the Article 29 Working Party as an example of when a DPIA should be carried out. Organisations should carry out a privacy impact assessment before starting to monitor their employees to clearly identify the purposes of monitoring, the benefit it is likely to deliver, the potential adverse impact of the monitoring arrangement, and to judge if monitoring is justified, as well as take into account the obligation that arises from monitoring. Organisations should also inform workers who are subject to the monitoring of the nature, extent and reasons for monitoring unless covert monitoring is justified.

Employers should also establish a policy on use by employees of electronic communications, explaining acceptable use of internet, phones and mobile devices, and the purpose and extent of electronic monitoring. It should also be outlined how the policy is enforced and the penalties for a breach of the policy.

Opening personal emails should be avoided where possible and should only occur where the reason is sufficient to justify the degree of intrusion involved.

47 ibid.
48 Article 29 Data Protection Working Party Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is ‘likely to result in a high risk’ for the purposes of Regulation 2016/679 – Adopted on 4 April 2017 – As last Revised and Adopted on 4 October 2017.
On 8 June 2017, the Article 29 Working Party adopted an opinion on data processing at work that also addressed employee monitoring. This opinion is unlikely to fundamentally change the ICO’s approach to employee monitoring in the United Kingdom. However, it does include a number of new recommendations, including that where it is possible to block websites rather than continually monitoring internet usage, employers should prefer prevention to detection.

iii Whistle-blowing hotlines

The use of whistle-blowing hotlines (where employees and other individuals can report misconduct or wrongdoing) is not prohibited by the DPA 2018 and their use is not restricted by the ICO. The ICO published guidance on the use of whistle-blowing hotlines in June 2017, where it noted that employees can notify the ICO where they believe the employer has not processed their personal data in accordance with data protection legislation. The ICO has not published updated guidance on the use of whistle-blowing hotlines after the entry into force of the GDPR and DPA 2018. However, organisations using whistle-blowing hotlines in the United Kingdom will have to comply with the data-protection principles under the DPA and the GDPR.

iv Electronic marketing

Under PECR, unsolicited electronic communications to individuals should only be sent with the recipient’s consent. The only exemption to this rule is known as ‘soft opt-in’, which will apply if the sender has obtained the individual’s details in the course of a sale or negotiations for a sale of a product or service; the messages are only marketing for similar products; and the person is given a simple opportunity to refuse marketing when his or her details are collected, and if he or she does not opt out, he or she is given a simple way to do so in future messages. These UK rules on consent do not apply to marketing emails sent to companies and other corporate bodies, such as a limited liability partnership, Scottish partnership or UK government body.

Senders of electronic marketing messages must provide the recipients with the sender’s name and a valid contact address.

The ICO has created a direct-marketing checklist, which enables organisations to check if their marketing messages comply with the law and which also proposes a guide to the

---

49 WP 249: Opinion 2/2017 on data processing at work, adopted 8 June 2017.
50 ICO, ‘Disclosures from whistleblowers’, 2 June 2017.
51 For guidance on how to comply with data protection principles under the DPA see WP 117: Opinion 1/2006 on the application of EU data protection rules to internal whistle-blowing schemes in the fields of accounting, internal accounting controls, auditing matters, and the fight against bribery, banking and financial crime adopted on 1 February 2006.
52 ICO, Guide to the Privacy and Electronic Communications Regulations, 2013, and Direct Marketing Guidance, V.2.2.
53 PECR Regulation 22(2).
55 PECR Regulation 23.
different rules on marketing calls, texts, emails, faxes and mail. The ICO has also published guidance on direct marketing, which it updated in March 2016.\textsuperscript{56} The ICO has launched a consultation phase on a Direct Marketing Code of Practice, which will replace the guidance.

In addition, the ICO has published on its website a guide on rules for businesses when marketing to other businesses under GDPR and PECR.\textsuperscript{57} It advises that the GDPR applies to individuals who can be identified either directly or indirectly, even when they are acting in a professional capacity. It also notes GDPR only applies to loose business cards where controllers intend to file them or input the details of the card into a computer system.

The proposed ePrivacy Regulation, which will have direct effect in the United Kingdom if it takes effect before the United Kingdom exits the European Union on 29 March 2019, will supersede the PECR. The current draft of the ePrivacy Regulation would require a higher standard of consent for direct marketing, equivalent to the consent standard in the GDPR. However, it is possible that existing exemptions such as the soft opt-in may be retained.\textsuperscript{58}

v Financial services

Financial services organisations, in addition to data protection requirements under the DPA 2018, also have legal and regulatory responsibilities to safeguard consumer data under rules of the UK Financial Conduct Authority (FCA), which includes having adequate systems and controls in place to discharge their responsibilities.

This includes financial services firms taking reasonable care to establish and maintain effective systems and controls for countering the risk that the firm might be used to further financial crime, such as by misuse of customer data.\textsuperscript{59}

Failure to comply with these security requirements may lead to the imposition of significant financial penalties by the FCA.

VII INTERNATIONAL TRANSFERS

The GDPR prohibits the transfer of personal data outside of the EEA to third countries (non-EEA Member State) unless:

\begin{itemize}
  \item[a] the recipient country is considered to offer an adequate level of data protection; or
  \item[b] a data protection safeguard has been applied (such as the EU’s standard contractual clauses for transfers of personal data from the EU also known as ‘model contracts’ or the organisation has implemented binding corporate rules); or
  \item[c] a derogation from the prohibition applies (such as the data subject has explicitly consented to the transfer).
\end{itemize}

This chapter does not consider the data protection safeguards and derogations in detail, which are set out in the EU chapter. However, it should be noted that under the DPA 1998, controllers were allowed to determine for themselves that their transfers of personal

\begin{itemize}
  \item[56] ICO, Direct Marketing Guidance, V.2.2.
  \item[57] ICO, For organisations/Marketing/The rules around business to business marketing, the GDPR and PECR, accessible at https://ico.org.uk/for-organisations/marketing/the-rules-around-business-to-business-marketing-the-gdpr-and-pecr/.
  \item[58] See the European Union overview chapter for more details on the proposed ePrivacy Regulation.
  \item[59] SYSC 3.
\end{itemize}
data outside of the EEA were adequately protected. The DPA 2018 does not contain such a self-adequacy assessment. However, the GDPR contains a more limited version of the DPA 1998 self-adequacy assessment, and allows transfers:

- that are not repetitive, concern only a limited number of data subjects and are necessary for the purposes of compelling legitimate interests that are not overridden by the interests or rights and freedoms of the data subject;
- where the controller has assessed all the circumstances surrounding the data transfer and has, as a result, implemented suitable data protection safeguards; and
- has notified the relevant data protection authority of the transfer.

The DPA 2018 also introduces a derogation where the transfer is a necessary and proportionate measure for the purposes of the controller’s statutory function.

In addition, the DPA 2018 also introduces further derogations for the transfer of personal data from the UK to a country outside of the EEA where the transfer is necessary for law enforcement purposes and is based on an adequacy decision.

If it is not based on an adequacy decision, it must be based on appropriate safeguards where a legal instrument containing appropriate safeguards for the protection of personal data binds the intended recipient of the personal data, or the data controller having assessed all the circumstances surrounding the transfers of that type of personal data to that specific country or territory outside of the EEA concludes that appropriate safeguards exist to protect the personal data. When relying on this particular derogation, the transfer must also be documented and such documents must be provided to the ICO upon request, including the date and time of the transfer, the name or any other pertinent information about the recipient, the justification for the transfer of the personal data; and a description of the personal data transferred.

If it is not based on an adequacy decision or on there being appropriate safeguards, it must be based on special circumstances that allow for the transfer of personal data from the UK to a country or territory outside of the EEA, where the transfer is necessary:

- to protect the vital interests of the data subject or another person;
- to safeguard the legitimate interests of the data subject;
- for the protection of an immediate and serious threat to the public security of a Member State or a third country;
- in individual cases for any law enforcement purposes, (provided the controller has not determined that fundamental rights and freedoms of the data subject override the public interest in the transfer of personal data from the UK to a third country); or
- in individual cases for a legal purpose (provided the controller has not determined that fundamental rights and freedoms of the data subject override the public interest in the transfer of personal data from the UK to a third country). When relying on this particular derogation, the transfer must also be documented and such documents must be provided to the ICO upon request, including the date and time of the transfer, the name or any other pertinent information about the recipient, the justification for the transfer of the personal data, and a description of the personal data transferred.
VIII DISCOVERY AND DISCLOSURE

The ICO has not published any specific guidance on this topic.\(^{60}\) E-discovery procedures and the disclosure of information to foreign enforcement agencies will, most of the time, involve the processing of personal data. As a result, organisations will have to comply with the data protection principles under the DPA 2018 in relation to e-discovery and must comply with the requirements of the GDPR.

In practice, this will mean informing data subjects about the processing of their personal data for this purpose. Organisations will also have to have a legal basis for processing the data.

A data transfer solution will also have to be implemented if the data is sent to a country outside the EEA that is not deemed to provide an adequate level of protection pursuant to Article 45 of the GDPR.

IX PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

The ICO has a range of enforcement powers under the DPA 2018, including monitoring and enforcement of the GDPR and the DPA 2018 in the UK. Such monitoring and enforcement powers include the power to issue:

a information notices: requiring controllers and processors to provide the ICO with information that the Commissioner reasonably requires in order to assess compliance with the GDPR or DPA 2018;

b assessment notices: requiring the controller or processor to permit the ICO to carry out an assessment of whether the controller or processor is in compliance with the GDPR or DPA 2018 (this may include the power of the ICO to conduct an audit, where the assessment notice permits the ICO to enter specified premises, inspect or examine documents, information, material and observe processing of personal data on the premises);

c notice of intent: where, after conducting its investigation, the ICO issues a notice of intent to fine the controller or processor in relation to a breach of the GDPR or the DPA 2018. Such a notice sets out the ICO’s areas of concern with respect to potential non-compliance of the GDPR or the DPA 2018 and grants the controller or processor the right to make representations. After such representations have been carefully considered, the ICO reaches its final decision on any enforcement action in the form of an enforcement notice;

d enforcement notices: such notices are issued where the ICO has concluded the controller or processor has failed to comply with the GDPR or the UK DPA 2018, setting out the consequences of non-compliance, which could include a potential ban on processing all or certain categories of personal data; and

e penalty notices: if the ICO is satisfied that the controller or processor has failed to comply with the GDPR or the DPA 2018 or has failed to comply with an information notice, an assessment notice or an enforcement notice, the ICO may, by written notice,

---

\(^{60}\) The Article 29 Working Party has, however, published a working document on this topic. See the European Union Overview chapter for more details.
require a monetary penalty to be paid for failing to comply with the GDPR or the DPA 2018. Under the GDPR, such monetary penalties can amount to €20 million or 4 per cent of annual worldwide turnover.

As the DPA 2018 came into effect on 23 May 2018, any information notices issued by the ICO to commence possible investigations, assessment notices or enforcement notices served pre-23 May 2018 and thus served under the Data Protection Act 1998, continue to have effect under the DPA 2018.

In a speech at the Data Protection Practitioners’ Conference on 9 April 2018, the ICO Information Commissioner, Elizabeth Dunham, stated that the ‘enforcement is a last resort’ and that she has ‘no intention of changing the ICO’s proportionate and pragmatic approach after 25th of May’. She added, ‘Hefty fines will be reserved for those organisations that persistently, deliberately or negligently flout the law’ and ‘those organisations that self-report, engage with us to resolve issues and can demonstrate effective accountability arrangements can expect this to be a factor when we consider any regulatory action’.

In addition, the ICO is responsible for promoting public awareness and in particular raising awareness among controllers and processors, of their obligations under the GDPR and DPA 2018.

The FCA also has enforcement powers and can impose financial penalties on financial services organisations for failure to comply with their obligations to protect customer data.

ii Recent ICO-led enforcement cases

Due to the GDPR and DPA 2018’s recent entry into force, all ICO’s published enforcement notices and monetary penalty notices at the time of writing, were issued under the DPA 1998.

In May 2018, the Crown Prosecution Service was fined £350,000 after losing historical child sex abuse victims interview videos, containing the most intimate sensitive details of the victims and perpetrator as well as identifying information pertaining to other parties.

In May 2018, a university was fined £120,000 for inadequate security measures following a cyberattack of a microsite that contained contact details and sensitive data of university employees and students. It was the first university to be fined under the DPA 1998.

In June 2018, a local police force was fined £80,000 by the ICO after sending a bulk email which contained sensitive personal data, identifying victims of historical child abuse.

In June 2018, the ICO fined a bible society £100,000 for inadequate technical and organisational measures that allowed their computer network to become compromised as a result of the cyberattack, with the cyberattacker able to access the personal data of 417,000 of the society’s supporters. A small subset of the supporters also had some payment card and bank account details placed at risk.

In June 2018, a global web service provider was fined £250,000 by the ICO for inadequate technical and organisational measures that allowed a cyberattacker to access personal data of approximately 500 million users.

X CONSIDERATIONS FOR FOREIGN ORGANISATIONS

The DPA 2018 applies to a data controller established in the United Kingdom and processing personal data in the context of that establishment, regardless of whether the processing takes place in the United Kingdom. It also applies to foreign organisations not established in the
UK, or in any other EEA state, that process personal data in relation to the offering of goods or services to data subjects in the UK or to the monitoring of data subjects in the UK, as far as their behaviour takes place in the UK. Data controllers not established in the United Kingdom or any other EEA country and processing personal data of data subjects in the UK must nominate a representative established in the UK and comply with the data principles and requirements under the GDPR and DPA 2018.

XI  CYBERSECURITY AND DATA BREACHES

i  Cybersecurity


The Investigatory Powers Act (IPA) received Royal Assent on 29 November 2016. The Act prohibits the interception of communications without lawful authority and sets out the situations in which there is lawful authority. Various law enforcement and intelligence authorities can, under the IPA, make targeted demands on telecommunications operators.

Under the IPA, the Secretary of State may by giving notice require a public telecommunications operator to retain communications data for a period that must not exceed 12 months if he or she considers that this is necessary and proportionate for one or more of the purposes for which communications may be obtained under the IPA. The IPA also expands the data retention requirements in the DRIP Act that it replaces (see below) to a broader range of communications data, such as site browsing histories.

The IPA is controversial and like its predecessor, the DRIP Act, which was an emergency piece of legislation and automatically expired on 31 December 2016, it has been criticised for lacking basic safeguards and for granting overly expansive powers for the bulk collection of data. The legality of the IPA has already been called into question following a ruling of the CJEU on the data retention provisions in the DRIP Act. One year after receiving Royal Assent, the English High Court issued a landmark judgment declaring the DRIP Act unlawful. The High Court ruled that a number of the provisions in the DRIP Act were incompatible with EU human rights law. However, the ruling was suspended until 31 March 2016 to give UK legislators time to implement appropriate safeguards. Preliminary questions were referred to the CJEU by the English Court of Appeal. On 21 December 2016, the CJEU issued a landmark ruling that effectively upheld an original decision of the High Court in relation to the validity of the provisions of the DRIP Act. Although the ruling concerned the DRIP Act, the IPA does little to address the criticisms of the DRIP Act in the CJEU’s judgment and in some cases provides for even more extensive powers than under the DRIP Act. The case was returned to the Court of Appeal, who in January 2018, issued its judgment, ruling the DRIP Act was incompatible with EU law as the DRIP Act did not restrict the accessing of communications data to ‘investigations of serious crime’ nor did requests by police or other public bodies to access communications data meet independent oversight by way of a ‘prior review by a court or independent administrative authority’. The UK government responded that it was making amendments to the IPA to take into account judicial criticisms of the DRIP Act. The UK High Court ruled in April 2018 that the UK government has six months to introduce changes to the IPA to make it compatible with UK law. It is clear that faced

61  Case C-698/15 Secretary of State for the Home Department v. Tom Watson, Peter Brice and Geoffrey Lewis.
with considerable judicial criticism the IPA needs further amendments; however, it is unclear whether these amendments will take the form of further primary legislation or a statutory instrument.


The interception powers in Part 1, Chapter 1 of RIPA have been repealed and replaced by a new targeted interception power under the IPA.

**UK cybersecurity strategy**

In November 2011, the Cabinet Office published the UK Cyber Security Strategy: Protecting and promoting the UK in a digital world, with four objectives for the government to achieve by 2015:

- **a** tackling cybercrime and making the United Kingdom one of the most secure places in the world to do business;
- **b** to be more resilient to cyberattacks and better able to protect our interests in cyberspace;
- **c** to create an open, stable and vibrant cyberspace that the UK public can use safely and that supports open societies; and
- **d** to have the cross-cutting knowledge, skills and capability it needs to underpin all our cybersecurity objectives.

In March 2013, the government launched the Cyber-security Information Sharing Partnership to facilitate the sharing of intelligence and information on cybersecurity threats between the government and industry.

The government has also developed the Cyber Essentials scheme, which aims to provide clarity on good cybersecurity practice.

Along with the Cyber Essentials scheme, the government has published the Assurance Framework, which enables organisations to obtain certifications to reassure customers, investors, insurers and others that they have taken the appropriate cybersecurity precautions. The voluntary scheme is currently open and available to all types of organisation.

In June 2015, the government launched a new online cybersecurity training course to help the procurement profession stay safe online.

In July 2015, the government announced the launch of a new voucher scheme to protect small businesses from cyberattacks, which will offer micro, small and medium-sized businesses up to £5,000 for specialist advice to boost their cybersecurity and protect new business ideas and intellectual property.

In January 2016, the government announced plans to assist start-ups offering cybersecurity solutions. Such start-ups will be given help, advice and support through the Early State Accelerator Programme, a £250,000 programme designed to assist start-ups in developing their products and bringing them to market. The programme is run by Cyber London and the Centre for Secure Information Technologies, and is funded by the government’s National Cyber Security Strategy programme.

In March 2016, the government announced that the United Kingdom’s new national cyber centre (announced in November 2015) would be called the National Cyber Security Centre (NCSC). The NCSC, which is based in London, opened in October 2016 and is intended to help tackle cybercrime.

In response to the European Parliament’s proposal for a NIS Directive in March 2014, which was part of the European Union’s Cybersecurity Strategy, and proposed certain
measures including new requirements for ‘operators of essential services’ and ‘digital service providers’, the UK government has implemented the NIS Directive into national law in the form of the UK Network and Information Systems Regulations 2018 (the NIS Regulations), which came into force on 10 May 2018.

The NIS Regulations have established a legal framework that imposes security and notification of security incident obligations on:

a. operators of essential services, being energy, transport, digital infrastructure, the health sector and drinking water supply and distribution services; and

b. on relevant digital service providers, being online marketplace providers, online search engines and cloud computing service providers.

The NIS Regulations also require the UK government to outline and publish a strategy to provide strategic objectives and priorities on the security of the network and information systems in the UK.

The NIS Regulations also imposes a tiered system of fines in proportion to the impact of the security incident, with a maximum fine of £17 million imposed where a competent authority decides the incident has caused or could cause an immediate threat to life or a significantly adverse impact on the UK economy.

Data controllers in the UK may in the event of a data security breach have to notify the relevant authorities both under the GDPR and the NIS Regulations.

Under the GDPR data controllers are required to report personal data breaches to the ICO without undue delay, unless the breach is unlikely to result in a risk to the rights and freedoms of the data subject. and, where feasible, no later than 72 hours after the controller becomes aware of the breach.\textsuperscript{62} If a controller does not report the data breach within 72 hours, it must provide a reasoned justification for the delay in notifying the ICO. The controller is also subject to a concurrent obligation to notify affected data subjects without undue delay when the notification is likely to result in a high risk to the rights and freedoms of natural persons.\textsuperscript{63} Under the GDPR, data processors also have an obligation to notify the data controller of personal data breaches without undue delay after becoming aware of a personal data breach.\textsuperscript{64}

According to the ICO, there should be a presumption to report a breach to the ICO if a significant volume of personal data is concerned and also where smaller amounts of personal data are involved but there is still a significant risk of individuals suffering substantial harm.\textsuperscript{65} The ICO have stated the 72-hour deadline to report a personal data breach includes evenings, weekends and bank holidays\textsuperscript{66} and where a controller is not able to report a breach within the 72-hour deadline, it must give reasons to the ICO for its delay.

As part of the notification, the ICO requires controllers to inform the ICO of:

\begin{itemize}
  \item[a] the number of data subjects affected by the personal data breach;
  \item[b] the type of personal data that has been affected;
\end{itemize}

\textsuperscript{62} Article 33(1) of the GDPR.
\textsuperscript{63} Article 34 of the Regulation.
\textsuperscript{64} Article 33(2) of the Regulation.
\textsuperscript{65} ICO, Guidance on Notification of Data Security Breaches to the Information Commissioner’s Office, 27 July 2012.
\textsuperscript{66} ICO, Personal Data Breach Reporting Webinar, 19 July 2018.
c the likely impact on the data subjects as a result of the personal data breach;
d steps the controller has taken to rectify the personal data breach and to ensure it does not happen again; and
e the name of the DPO or another point of contact for the ICO to request further information.

The GDPR also imposes a requirement on controllers to inform the data subject where the personal data breach represents a high risk to their rights and freedoms. The ICO, in a webinar in July 2018, stated it was of the view that the threshold is higher for informing data subjects of the personal data breach than it is for informing the ICO of the personal data breach. According to the ICO, this is because the aim of informing data subjects is so that they can take action to protect themselves in the event of a personal data breach. Therefore, informing them of every personal data breach, regardless of whether it has an effect on the data subject, can lead to notification fatigue, where the consequences of the breach are relatively minor.

In addition, when notification is given to the ICO of the personal data breach, the ICO can also require the controller to inform the data subjects of the personal data breach.

In addition, under the PECR and the Notification Regulation, internet and telecommunication service providers must report breaches to the ICO no later than 24 hours after the detection of a personal data breach where feasible. The ICO has published guidance on this specific obligation to report breaches.

XII OUTLOOK

The UK departs the European Union on 29 March 2019, but there is no legally binding transition agreement, at present, that will determine the nature and content of any transitional agreement, in particular, in relation to the processing of personal data between the UK and the EU.

As the GDPR is a regulation, it has direct effect in UK law. As the GDPR came into force prior to the UK’s scheduled departure from the EU its data protection obligations will continue to have legal effect post-Brexit, unless the UK government decides to introduce legislation repealing the provisions and legal effect of the GDPR in UK law and amend the provisions of the DPA 2018.

67 ibid.
68 PECR Regulation 5A(2).
70 Article 2 of the Notification Regulation. The content of the notification is detailed in Annex 1 to the Notification Regulation.
In relation to the processing and transfer of personal data between the UK and the EU, the UK government has proposed a ‘bespoke adequacy agreement’ between the EU and the UK. Under the agreement, the current adequacy framework provided by the European Commission should be extended to include:

- a clear and transparent framework to facilitate dialogue between the UK and the EU, minimise the risk of disruption to data flows and support a stable relationship between the UK and the EU to protect the personal data of UK and EU data subjects; and
- greater regulatory cooperation and enforcement action between the ICO and EU Member State data supervisory authorities.

The Information Commissioner, Elizabeth Denham, has stated that ‘there is no doubt that achieving a treaty arrangement or an adequacy decision with the EU represents the simplest way of ensuring the continued frictionless flow of data between the EU and the UK’. More generally, it is expected the ICO will continue to publish guidance on the GDPR and DPA 2018 during 2018 and beyond.

---


74 ‘Building the cybersecurity community’, Elizabeth Denham, National Cyber Security Centre’s CYBERUK 2018 event, 12 April 2018.
I OVERVIEW

Although not universally acknowledged, the US commercial privacy regime is arguably the oldest, most robust, well developed and effective in the world. The US privacy system has a relatively flexible and non-prescriptive nature, relying more on post hoc government enforcement and private litigation, and on the corresponding deterrent value of such enforcement and litigation, than on detailed prohibitions and rules. With certain notable exceptions, the US system does not apply a ‘precautionary principle’ to protect privacy, but rather allows injured parties (and government agencies ) to bring legal action to recover damages for, or enjoin a party from, ‘unfair or deceptive’ business practices. However, US federal law does impose affirmative prohibitions and restrictions in certain commercial sectors, such as those involving financial and medical data, and electronic communications, as well as with respect to children’s privacy, background investigations and ‘consumer reports’ for credit or employment purposes, and certain other specific areas. State laws add numerous additional privacy requirements.

Legal protection of privacy in civil society has been recognised in US common law since 1890, when the article ‘The Right to Privacy’ was published in the Harvard Law Review by Professors Samuel D Warren and Louis D Brandeis. Moreover, from its conception by Warren and Brandeis, the US system for protecting privacy in the commercial realm has been focused on addressing technological innovation. The Harvard professors astutely noted that ‘[r]ecent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual [. . .] the right “to be let alone”.’ In 1974, Congress enacted the federal Privacy Act, regulating government databases, and found that ‘the right to privacy is a personal and fundamental right protected by the Constitution of the United States’. It is generally acknowledged that the US Privacy Act represented the first official embodiment of the fair information principles and practices that have been incorporated in many other data protection regimes, including the European Union’s 1995 Data Protection Directive.

1 Alan Charles Raul is a partner at Sidley Austin LLP. Vivek K Mohan was previously an associate and is now senior privacy and cybersecurity counsel at Apple Inc. His work on the chapter predated his tenure at Apple. The authors wish to thank Tasha D Manoranjan and Frances E Faircloth, who were previously associates at Sidley, for their contributions to this chapter and prior versions. Passages of this chapter were originally published in ‘Privacy and data protection in the United States’, The debate on privacy and security over the network: Regulation and markets, 2012, Fundación Telefónica; and Raul and Mohan, ‘The Strength of the U.S. Commercial Privacy Regime’, 31 March 2014, a memorandum to the Big Data Study Group, US Office of Science and Technology Policy.
The United States has also led the way for the world not only in establishing model legal data protection standards in the 1974 Privacy Act, but also in terms of imposing affirmative data breach notification and information security requirements on private entities that collect or process personal data from consumers, employees and other individuals. The state of California was the path-breaker on data security and data breach notifications by first requiring in 2003 that companies notify individuals whose personal information was compromised or improperly acquired. Since then, all 50 states, the District of Columbia and other US jurisdictions, and the federal banking, healthcare and communications agencies, have also required companies to provide mandatory data breach notifications to affected individuals, and have imposed affirmative administrative, technical and physical safeguards to protect the security of sensitive personal information. Dozens of other medical and financial privacy laws also exist in various states. There is, however, no single omnibus federal privacy law in the United States. Moreover, there is no designated central data protection authority in the United States, although the Federal Trade Commission (FTC) has primarily assumed that role for consumer privacy. The FTC is independent of the President, and is not obliged (although it is encouraged) to respect the Administration’s perspective on the proper balance between costs and benefits with respect to protecting data privacy. The Chair of the FTC is designated by the President, however, and may be removed as Chair (although not as one of the FTC’s five commissioners) at the discretion of the President.

As in the EU and elsewhere, privacy and data protection are balanced in the United States in accordance with other rights and interests that societies need to prosper and flourish, namely economic growth and efficiency, technological innovation, property and free speech rights and, of course, the values of promoting human dignity and personal autonomy. The most significant factor in counterbalancing privacy protections in the United States, perhaps, is the right to freedom of expression guaranteed by the First Amendment. Preserving free speech rights for everyone certainly entails complications for a ‘right to be forgotten’, since one person’s desire for oblivion may run counter to another’s sense of nostalgia (or some other desire to memorialise the past for good or ill).

The First Amendment has also been interpreted to protect people’s right to know information of public concern or interest, even if it trenches to some extent on individual privacy. Companies have also been deemed to have a First Amendment right to communicate relatively freely with their customers by exchanging information in both directions (subject to the information being truthful, not misleading and otherwise not the subject of an unfair or deceptive business practice).

The dynamic and robust system of privacy governance in the United States marshals the combined focus and enforcement muscle of the FTC, state attorneys general, the Federal Communications Commission (FCC), the Securities and Exchange Commission (SEC), the Consumer Financial Protection Bureau (and other financial and banking regulators), the Department of Health and Human Services, the Department of Education, the judicial system, and last – but certainly not least – the highly motivated and aggressive US private plaintiffs’ bar. Taken together, this enforcement ecosystem has proven to be nimble, flexible and effective in adapting to rapidly changing technological developments and practices, responding to evolving consumer and citizen expectations, and serving as a meaningful agent

---

of deterrence and accountability. Indeed, the US enforcement and litigation-based approach appears to be particularly well suited to deal with ‘recent inventions and business methods’ – namely new technologies and modes of commerce – that pose ever-changing opportunities and unpredictable privacy challenges.

II THE YEAR IN REVIEW

Privacy and cybersecurity remain hot topics for regulators, and the past years have seen a number of agencies that previously exercised a limited mandate in this area issue guidance and pursue enforcement actions. The courts have also been active, and a number of recent cases promise to reshape the legal landscape for years to come.

As detailed below, the FTC has continued to play a leading role at the federal level on these issues. Other government agencies announced their focus on these issues, often issuing guidance for entities that fall within their regulatory sphere of influence. The SEC has exercised increasingly aggressive oversight regarding cybersecurity compliance and practices of broker-dealers and investment advisers. It announced exam priorities, and brought an enforcement action against an investment adviser that failed to maintain cybersecurity policies and procedures. The Department of Justice has also issued guidance for addressing data breach incidents, and for interacting with federal law enforcement.

At the end of 2017, the FCC adopted the Restoring Freedom Order, which reclassified broadband internet back to being an ‘information service,’ and thus not a common carrier service. This returned jurisdiction to the FTC to regulate ISPs under its Section 5 authority to protect consumers and promote competition, including ISP privacy practices. In January 2018, following adoption of the Restoring Internet Freedom Order, the FTC and FCC entered a memorandum of understanding, through which the agencies will coordinate online consumer protection as they did prior to the 2015 order.

States have continued to push privacy and cybersecurity initiatives forward. South Dakota and Alabama became the 49th and 50th states to enact data breach notification laws in 2018. The South Dakota law requires notice within 60 days of the discovery of a breach. Notice to individuals is not required where there is no significant risk of identity theft, but notice must still be given to the state’s attorney general. The Alabama law requires companies to provide Alabama residents with notification of a breach within 45 days of discovery. Notification is triggered by a determination of a breach that poses a risk of harm to impacted individuals. Other states, including Arizona, Colorado, Louisiana, and Oregon, have updated their notification laws.

On 28 June 2018, the California Consumer Privacy Act of 2018 (CCPA) was signed into law by that state’s governor. It is scheduled to go into effect on 1 January 2020, whereupon it may become the most far-reaching privacy or data protection law in the country. In many ways, the CCPA emulates the EU’s General Data Protection Regulation (GDPR). It mandates greater transparency and user control over data by imposing highly detailed disclosure requirements on companies that collect personal data about California residents. Unlike GDPR, however, CCPA generally permits opt-out rather than opt-in consent and it does not prohibit specific practices. The California law does mandate data subject rights regarding disclosure, access, and deletion. While it is anticipated that the CCPA will be subject to both legislative amendment (to correct errors and excesses) and regulatory interpretation (by the State Attorney General) before it takes effect in 2020, it may nonetheless influence
the development of other federal and state privacy legislation around the US. For example, California was the first state to enact data breach notification legislation, which all other states then followed.

On 16 May 2017, Washington became the third state to pass a law regulating biometric data, which governs the collection, use and retention of ‘biometric identifiers’, including fingerprints, voice prints, eye retinas, irises, or other patterns or characteristics that can be used to identify someone. The law specifically excludes ‘physical or digital photograph, video or audio recording or data generated therefrom’ (in addition to certain health-related data), suggesting the statute will have limited application in the context of facial-recognition technology. The law restricts the sale, lease and other disclosure of the data and requires its protection, but like a similar law in Texas, it does not provide for a private right of action. Illinois, the other state to pass a biometric data law, does, however, provide for a private cause of action, which has already spawned some litigation. Other states, including Connecticut, New Hampshire and Alaska, have considered the regulation of biometric data.

One case that saw continued development in early 2017 was *Spokeo, Inc v. Robins*. Thomas Robins had sued Spokeo for wilful violations of the Fair Credit Reporting Act (FCRA), alleging that inaccurate information disclosed about him on Spokeo’s website harmed his employment opportunities. In May 2016, the Supreme Court remanded the case to the Ninth Circuit for consideration of whether Robins had suffered an injury that was sufficiently ‘concrete’ to find standing. On remand from the Supreme Court, on 15 August 2017, the Ninth Circuit held that an alleged injury was sufficiently ‘concrete’, citing the harms that may arise when persons’ personal information is misused or improperly accessed. On 22 January 2018, the United States Supreme Court declined to review the Ninth Circuit Court of Appeals’ decision.

In data breach litigation, courts continue to disagree about whether plaintiffs should prevail where they cannot allege that the criminal actually misused stolen data. In August 2017, the DC Circuit held that plaintiffs making allegations related to a 2015 breach had plausibly alleged a risk of harm, even without proving that their potentially stolen social security numbers had already been misused. Meanwhile, the Eighth Circuit held – on the one hand – that a plaintiff had standing to sue a company after a breach based on the theory that the plaintiff had paid for a certain level of security, and thus, the plaintiff arguably did not get the value of that bargain. On the other hand, however, the same court held that the case should be dismissed for failure to state a claim because of lack of evidence that anyone actually suffered fraud or identity theft resulting in financial loss. Moreover, the court stated that: ‘[t]he implied premise that because data was hacked [the company’s] protections must have been inadequate is a “naked assertion devoid of further factual enhancement” that cannot survive a motion to dismiss’ and ‘massive class action litigation should be based on more than allegations of worry and inconvenience’.

Amid this uncertainty, large-scale breaches and attacks continue to occur. On 12 May 2017, the WannaCry attack disabled computers in organisations across the world, including the UK National Health Service. Hackers, believed to be in North Korea, demanded money to unfreeze the computers. WannaCry exploited weaknesses in unpatched Windows XP operating systems and wreaked havoc in the United States, the United Kingdom and around the world. On 7 September 2017, Equifax, one of the three major consumer credit reporting agencies, announced that it had suffered a hack that potentially compromised the
data of 143 million Americans. In 2018, a variety of websites including MyFitnessPal, a fitness app run by Under Armour; Ticketmaster; and numerous other companies publicly reported cybersecurity incidents.

i FTC actions

In October 2016, the FTC announced the release of a new guide for businesses dealing with data breaches. The guide covers the process businesses should follow and what officials they should contact when there is a data breach. It includes advice regarding secure systems, managing service providers, segmenting networks and notifying users whose information has been stolen. The FTC also released a video explaining much of the same material.

On 6 February 2017, the FTC announced that VIZIO had agreed to pay US$2.2 million to settle charges by the FTC and the New Jersey attorney general that it installed software on TVs to collect viewing data of its 11 million customers without their knowledge or consent. The order required VIZIO to prominently disclose and obtain affirmative express consent for data collection and sharing. The settlement also required VIZIO to delete all data it collected before 1 March 2016 and to implement a comprehensive data privacy programme that would be regularly assessed.

On 15 August 2017, the FTC reached a settlement with Uber regarding allegations that the company had misrepresented its cybersecurity protections and engaged in unreasonable cybersecurity practices. The settlement sheds greater light on what the FTC means by the ‘reasonable data security’ measures it expects companies to take. Uber suffered a breach of its drivers’ location and other data and was the subject of 2014 news reports that alleged Uber employees could gain access to and use its customers’ personal information, including precise geolocation data. The FTC settlement clarified the core elements of a ‘reasonable’ data security programme, including restricted employee access to sensitive data, multi-factor authentication for remote access and encryption of sensitive personal data both in transit and at rest.

The Court of Justice of the European Union (CJEU) has had an outsize impact on privacy and data protection issues that affect US companies. The CJEU decision invalidating the US–EU Safe Harbor in October 2015 led to lengthy negotiations between US and EU authorities on an appropriate replacement mechanism for data transfers across the Atlantic, resulting in the EU–US Privacy Shield Framework (Privacy Shield), which has been in place for more than a year. The FTC has brought three recent enforcement actions alleging that companies made false claims about Privacy Shield participation. In all three complaints, the FTC alleged the companies falsely stated in their privacy policies that they would comply with Privacy Shield, because the companies started the application for Privacy Shield compliance but did not complete the necessary steps to ensure full compliance before claiming they were Privacy Shield participants.

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

The United States has specific privacy laws for the types of citizen and consumer data that are most sensitive and at risk:

- financial, insurance and medical information;
- information about children and students;
- telephone, internet and other electronic communications and records;
Moreover, the United States is the unquestioned world leader in mandating information security and data breach notifications, without which information privacy is not possible. If one of the sector-specific federal or state laws does not cover a particular category of data or information practice, then the Federal Trade Commission Act (FTCA), and each state’s ‘little FTCA’ analogue, comes into play. Those general consumer protection statutes broadly, flexibly and comprehensively proscribe (and authorise tough enforcement against) unfair or deceptive acts or practices. The FTC is the de facto privacy regulator in the United States. State attorneys general and private plaintiffs can also enforce privacy standards under analogous ‘unfair and deceptive acts and practices’ standards in state law. Additionally, information privacy is further protected by a network of common law torts, including invasion of privacy, public disclosure of private facts, ‘false light’, appropriation or infringement of the right of publicity or personal likeness, and, of course, remedies against general misappropriation or negligence. In short, there are no substantial lacunae in the regulation of commercial data privacy in the United States. In taking both a general (unfair or deceptive) and sectoral approach to commercial privacy governance, the United States has empowered government agencies to oversee data privacy where the categories and uses of data could injure individuals.

**FTCA**

Section 5 of the FTCA prohibits ‘unfair or deceptive acts or practices in or affecting commerce’. While the FTCA does not expressly address privacy or information security, the FTC applies Section 5 to information privacy, data security, online advertising, behavioural tracking and other data-intensive, commercial activities. The FTC has brought successful enforcement actions under Section 5 against companies that failed to adequately disclose their data collection practices, failed to abide by the promises made in their privacy policies, failed to comply with their security commitments or failed to provide a ‘fair’ level of security for consumer information.

Under Section 5, an act or practice is deceptive if there is a representation or omission of information likely to mislead a consumer acting reasonably under the circumstances; and the representation or omission is ‘material’ – defined as an act or practice ‘likely to affect the consumer’s conduct or decision with regard to a product or service’. An act or practice is ‘unfair’ under Section 5 if it causes or is likely to cause substantial injury to consumers that is not reasonably avoidable and lacks countervailing benefits to consumers or competition.

The FTC takes the position that companies must disclose their privacy practices adequately, and that in certain circumstances, this may require particularly timely, clear and prominent notice, especially for novel, unexpected or sensitive uses. The FTC brought an enforcement action in 2009 against Sears for allegedly failing to adequately disclose the extent to which it collected personal information by tracking the online browsing of consumers who downloaded certain software. The consumer information allegedly collected included ‘nearly all of the Internet behavior that occurs on [. . .] computers’. The FTC required Sears to prominently disclose any data practices that would have significant unexpected implications in a separate screen outside any user agreement, privacy policy or terms of use.
Section 5 is also generally understood to prohibit a company from using previously collected personal data in ways that are materially different from, and less protective than, what it initially disclosed to the data subject, without first obtaining the individual’s additional consent.

The FTC staff has also issued extensive guidance on online behavioural advertising, emphasising four principles to protect consumer privacy interests:

a. transparency and control, giving meaningful disclosure to consumers, and offering consumers choice about information collection;

b. maintaining data security and limiting data retention;

c. express consent before using information in a manner that is materially different from the privacy policy in place when the data were collected; and

d. express consent before using sensitive data for behavioural advertising.

The FTC’s report does not, however, require opt-in consent for the use of non-sensitive information in behavioural advertising.

Fair information practice principles

The innovative American privacy doctrine elaborated theories for tort and injunctive remedies for invasions of privacy (including compensation for mental suffering). The Warren–Brandeis right to privacy, along with the right to be let alone, was followed in 1973 by the first affirmative government undertaking to protect privacy in the computer age. The new philosophy was expressed in the Report of the Secretary’s Advisory Committee on Automated Personal Data Systems, published by the US Department of Health, Education, and Welfare (HEW) (now the Department of Health and Human Services). This report developed the principles for ‘fair information practices’ that were subsequently adopted by the United States in the 1974 Privacy Act, and ultimately by the European Union in 1995 in its Data Protection Directive. The fair information practice principles established in the United States in 1973–1974 remain largely operative around the world today in regimes and societies that respect information privacy rights of individuals. The fundamental US HEW/Privacy Act principles were:

a. there must be no personal data record-keeping systems whose very existence is secret;

b. there must be a way for an individual to find out what information about him or her is in a record and how it is used;

c. there must be a way for an individual to prevent information about him or her obtained for one purpose from being used or made available for other purposes without his or her consent;

d. there must be a way for an individual to correct or amend a record of identifiable information about him or her; and

e. any organisation creating, maintaining, using or disseminating records of identifiable personal data must assure the reliability of the data for their intended use, and must take reasonable precautions to prevent misuse of the data.

Classification of data

The definitions of personal data and sensitive personal data vary by regulation. The FTC considers information that can reasonably be used to contact or distinguish an individual (including IP addresses) to constitute personal data (at least in the context of children's
privacy). Generally, sensitive data includes personal health data, credit reports, personal information collected online from children under 13, precise location data, and information that can be used for identity theft or fraud.

**Federal laws**

Congress has passed laws protecting personal information in the most sensitive areas of consumer life, including health and financial information, information about children and credit information. Various federal agencies are tasked with rule making, oversight and enforcement of these legislative directives.

The scope of these laws and the agencies that are tasked with enforcing them is formidable. Laws such as the Children’s Online Privacy Protection Act of 1998 (COPPA), the Health Insurance Portability and Accountability Act of 1996, the Financial Services Modernization Act of 1999 (Gramm-Leach-Bliley Act or GLBA), the FCRA, the Electronic Communications Privacy Act, the Communications Act (regarding CPNI) and the Telephone Consumer Protection Act of 1991, to name just a few, prescribe specific statutory standards to protect the most sensitive consumer data.

The Cybersecurity Act, passed in 2015, includes a Cybersecurity Information Sharing Act (CISA). CISA is designed to foster cyberthreat information sharing and to provide certain liability shields related to such sharing and other cyber-preparedness. In addition, US intelligence agency collection of bulk phone metadata pursuant to the USA Freedom Act ended in 2015, which means that targeted court orders are required for government collection of phone metadata stored by telecommunications companies.

The Defend Trade Secrets Act (DTSA) also provides federal legislative protection for information by expanding access to judicial redress for unauthorised access and use of trade secrets. The DTSA amends the Economic Espionage Act of 1996 to provide plaintiffs with a private cause of action to sue for trade-secret theft and pursue damages in federal court. The DTSA authorises a federal court to grant an injunction to prevent actual or threatened misappropriation of trade secrets, but the injunction may not prevent a person from entering into an employment relationship; nor place conditions on employment based merely on information the person knows. Rather, any conditions placed on employment must be ‘based on evidence of threatened misappropriation’. Moreover, the DTSA precludes the court from issuing an injunction that would ‘otherwise conflict with an applicable state law prohibiting restraints on the practice of a lawful profession, trade or business’.

**State laws**

In addition to the concurrent authority that state attorneys general share for enforcement of certain federal privacy laws, state legislatures have been especially active on privacy issues that states view worthy of targeted legislation. In the areas of online privacy and data security alone, state legislatures have passed laws covering a broad array of privacy-related issues,\(^3\)

cyberstalking, data disposal, privacy policies, security breach notification, employer access to employee social media accounts, unsolicited commercial communications and electronic solicitation of children, to name but a few.

California is viewed as a leading legislator in the privacy arena, and its large population and high-tech sector means that the requirements of California law receive particular attention and often have de facto application to businesses operating across the United States.

The highly significant, new California Consumer Privacy Act of 2018 is discussed above in Section II.

**Co-regulation and industry self-regulation**

To address concerns about privacy practices in various industries, industry stakeholders have worked with the government, academics and privacy advocates to build a number of co-regulatory initiatives that adopt domain-specific, robust privacy protections that are enforceable by the FTC under Section 5 and by state attorneys general pursuant to their concurrent authority. These cooperatively developed accountability programmes establish expected practices for use of consumer data within their sectors, which is then subject to enforcement by both governmental and non-governmental authorities. This approach has had notable success, such as the development of the ‘About Advertising’ icon by the Digital Advertising Alliance and the opt-out for cookies set forth by the Network Advertising Initiative. Companies that assert their compliance with, or membership in, these self-regulatory initiatives must comply with these voluntary standards or risk being deemed to have engaged in a deceptive practice. The same is true for companies that publish privacy policies – a company’s failure to comply with its own privacy policy is a quintessentially deceptive practice. It should also be noted that various laws require publication or provision of privacy policies, including, inter alia, the GLBA (financial data), Health Insurance Portability and Accountability Act (HIPAA) (health data) and California law (websites collecting personal information). In addition, voluntary membership or certification in various self-regulatory initiatives also require posting of privacy policies, which then become enforceable by the FTC, state attorneys general and private plaintiffs claiming detrimental reliance on those policies.

**ii General obligations for data handlers**

There is no general requirement to register databases in the United States. Depending on the context, data handlers may be required to provide data subjects with a pre-collection notice, and the opportunity to opt out of the use and disclosure of regulated personal information.

---

10 See oag.ca.gov/privacy/privacy-laws.
11 See www.aboutads.info; www.networkadvertising.org/choices/?partnerId=1//.
Information that is considered sensitive personal information, such as health information, may involve opt-in rules. The FTC considers it a deceptive trade practice if a company engages in materially different uses or discloses personal information not disclosed in the privacy policy under which personal information was obtained.

iii Technological innovation and privacy law

Electronic marketing is extensively regulated in the United States through a myriad of laws. The CAN-SPAM Act is a federal law governing commercial email messages. Generally, a company is permitted to send commercial emails to anyone under CAN-SPAM, provided these conditions are met: the recipient has not opted out of receiving such emails from the company, the email identifies the sender and the sender’s contact information, and the email has instructions on how to easily and at no cost opt out of future commercial emails from the company.

Generally, express written consent is required for companies to send marketing text messages. Marketing texts are a significant class action risk area.

There is no specific federal law that regulates the use of cookies and other similar online tracking tools. However, the use of tracking mechanisms should be carefully and fully disclosed in a company’s website privacy policy. Additionally, it is best practice for websites that allow online behavioural advertising to participate in the Digital Advertising Alliance code of conduct, which enables users to easily opt out of being tracked for these purposes. California law imposes further requirements on online tracking. California requires companies that track personally identifiable information over time and multiple websites to disclose how the company responds to ‘do-not-track’ signals, and whether users can opt out of such tracking.

Location tracking is currently a subject of interest and debate. FCC regulations govern the collection and disclosure of certain location tracking by telecommunications providers (generally speaking, telephone carriers). Additionally, the FTC and California have issued best-practice recommendations for mobile apps and mobile app platforms.

iv Specific regulatory areas

The US system of privacy is composed of laws and regulations that focus on particular industries (financial services, healthcare, communications), particular activities (i.e., collecting information about children online) and particular types of data.

Federal

Financial privacy

For financial privacy, the federal banking agencies and the FTC were previously primarily responsible for enforcing consumer privacy under the GLBA, which applies to financial institutions. Following the 2010 Dodd-Frank legislation, such laws will be primarily (but not exclusively) enforced by the new Consumer Financial Protection Bureau, which has significant, independent regulatory and enforcement powers. The FTC, however, will remain primarily responsible for administering the FCRA, along with the general unfair and deceptive acts and practices standards under the FTCA and COPPA, which impose affirmative privacy and security duties on entities that collect personal information from children under 13 years of age.
The GLBA addresses financial data privacy and security by establishing standards for safeguarding customers’ ‘non-public personal information’ – or personally identifiable financial information – stored by ‘financial institutions’, and by requiring financial institutions to provide notice of their information-sharing practices. In brief, the GLBA requires financial institutions to provide notices of policies and practices regarding disclosure of personal information; to prohibit the disclosure of such data to unaffiliated third parties, unless consumers are provided the right to opt out of such disclosure or other exceptions apply; and to establish safeguards to protect the security of personal information.

The FCRA, as amended by the Fair and Accurate Credit Transactions Act of 2003, imposes requirements on entities that possess or maintain consumer credit reporting information, or information generated from consumer credit reports. Consumer reports are ‘any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer’s creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer’s eligibility’ for credit, insurance, employment or other similar purposes. The FCRA mandates accurate and relevant data collection to give consumers the ability to access and correct their credit information, and limits the use of consumer reports to permissible purposes such as employment, and extension of credit or insurance.

The Consumer Financial Protection Bureau (CFPB), which is the primary federal regulator of consumer financial products and services, brought its first data security enforcement action in 2016 under the authority granted by Dodd-Frank against Dwolla Inc, an online payments company, for allegedly deceptive representations with respect to its data security practices. Dodd-Frank authorises the CFPB to take action against institutions engaged in unfair, deceptive or abusive acts or practices or that otherwise violate federal consumer financial laws. Under the terms of the CFPB order against Dwolla, the company was required to stop misrepresenting its data security practices, train employees properly and fix security flaws. In addition, Dwolla was required to pay a US$100,000 civil money penalty.

On 18 October 2017, the CFPB released a set of consumer protection principles principles designed to protect consumer interests in the market for services built around consumer-approved use of financial information. The Principles are targeted to so-called ‘data aggregation’ or ‘screen scraping’ services that collect customer information in order to provide financial planning or other services. Over the past few years, data aggregation services and banks have struggled to develop the right model for sharing customer account data. The Principles issued by the CFPB seek to provide a potential data-sharing model for banks and data aggregation services while protecting consumer interests. Although the Principles set forth by the CFPB are not binding requirements, they signal increased momentum for a workable model of data sharing between banks and fintech companies. They may also demonstrate the CFPB’s expectations of market participants and its broader viewpoints about consumer privacy and consent. The nine Principles cover the areas of data access, data scope and usability, consumer control and informed consent, separate authorisation credentials, data security, access transparency, data accuracy, consumer ability to dispute and resolve unauthorised access, and efficient and effective accountability mechanisms for risks.

**Healthcare privacy**

For healthcare privacy, agencies within the Department of Health and Human Services administer and enforce HIPAA, as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH). HIPAA was enacted to create national standards for electronic healthcare transactions, and the US Department of Health and Human Services has promulgated regulations to protect privacy and security of personal health information (PHI). Patients generally have to opt in before their information can be shared with other organisations. HIPAA applies to ‘covered entities’, which include health plans, healthcare clearing houses and healthcare providers that engage in electronic transactions as well as, via HITECH, service providers to covered entities that need access to PHI to perform their services. It also imposes requirements in connection with employee medical insurance.

‘Protected health information’ is defined broadly as ‘individually identifiable health information [. . .] transmitted or maintained in electronic media’ or in ‘any other form or medium’. ‘Individually identifiable health information’ is defined as information that is a subset of health information, including demographic information that ‘is created or received by a health care provider, health plan, employer, or health care clearinghouse’; that ‘relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual’; and that either identifies the individual or provides a reasonable means by which to identify the individual. HIPAA also does not apply to ‘de-identified’ data.

A ‘business associate’ is an entity that performs or assists a covered entity in the performance of a function or activity that involves the use or disclosure of PHI (including, but not limited to, claims processing or administration activities). Business associates are required to enter into agreements, called business associate agreements, requiring business associates to use and disclose PHI only as permitted or required by the business associate agreement or as required by law, and to use appropriate safeguards to prevent the use or disclosure of PHI other than as provided for by the business associate agreement, as well as numerous other provisions regarding confidentiality, integrity and availability of electronic PHI. HIPAA and HITECH not only restrict access to and use of medical information, but also impose stringent information security standards.

**Communications privacy**

For communications privacy, the FCC, the Department of Justice and, to a considerable extent, private plaintiffs can enforce the data protection standards in the Electronic Communications Privacy Act, the Computer Fraud and Abuse Act and various sections of the Communications Act, which include specific protection for CPNI such as telephone call records. The Electronic Communications Privacy Act of 1986 protects the privacy and security of the content of certain electronic communications and related records. The Computer Fraud and Abuse Act prohibits hacking and other forms of harmful and unauthorised access or trespass to computer systems, and can often be invoked against disloyal insiders.

---

or cybercriminals who attempt to steal trade secrets or otherwise misappropriate valuable corporate information contained on corporate computer networks. The FCC, however, is the primary regulator for communications privacy issues, and has been active over the past year.

The FCC shares jurisdiction with the FTC on certain privacy and data security issues, including notably on the issue of robocalls as governed by the Telephone Consumer Protection Act. There has been significant regulatory activity in the past year, including guidance released by the FCC on auto-diallers in August 2015, not to mention substantial private litigation driven by the statutory penalties provided for by the Telephone Consumer Protection Act (TCPA). The FCC has stated that complaints regarding unwanted calls are the largest category of complaints received by the FCC – numbering over 215,000 complaints in 2014 alone.14

Children’s privacy

COPPA applies to operators of commercial websites and online services that are directed to children under the age of 13, as well as general audience websites and online services that have actual knowledge that they are collecting personal information from children under the age of 13. COPPA requires that these website operators post a privacy policy, provide notice about collection to parents, obtain verifiable parental consent before collecting personal information from children, and other actions.15

Other federal privacy laws

Even the array of privacy laws described above is hardly comprehensive. A number of other federal privacy laws protect personal information in the areas of cable television, education, telecommunications customer information, drivers’ and motor vehicle records, and video rentals. Federal laws also protect marketing activities such as telemarketing, junk faxes and unsolicited commercial email. In addition, in October 2016, the Department of Transportation issued guidance on cybersecurity best practices for interconnected cars and self-driving technology.

State legislation

In the areas of online privacy and data security alone, state legislatures have passed a number of laws covering access to employee and student social media passwords, children’s online privacy, e-Reader privacy, online privacy policies, false and misleading statements in website privacy policies, privacy of personal information held by ISPs, notice of monitoring of employee email communications and internet access, phishing, spyware, security breaches, spam and event data recorders. California is viewed as the leading legislator in the privacy arena, with many other states following its privacy laws. State attorneys general also have concurrent authority with the FTC or other federal regulators under various federal laws, such as COPPA, HIPAA and others.

The National Council of State Legislatures summarises the following state provisions regarding online privacy:

15 Available at www.law.cornell.edu/USCode/text/15/6501.
**Privacy Policies for Websites or Online Services**

California's Online Privacy Protection Act requires an operator [. . .] to post a conspicuous privacy policy on its Website or online service [. . .] and to comply with that policy. The law, among other things, requires that the privacy policy identify the categories of personally identifiable information that the operator collects about individual consumers who use or visit its Website [and] how the operator responds to a web browser 'Do Not Track' signal. Connecticut [r]quires any person who collects Social Security numbers in the course of business to create a privacy protection policy. The policy must be 'publicly displayed' by posting on a web page and the policy must [. . .] protect the confidentiality of Social Security numbers.

**Privacy of Personal Information Held by Internet Service Providers**

Two states, Nevada and Minnesota, require Internet Service Providers to keep private certain information concerning their customers, unless the customer gives permission to disclose the information. Both states prohibit disclosure of personally identifying information, but Minnesota also requires ISPs to get permission from subscribers before disclosing information about the subscribers' online surfing habits and Internet sites visited.

**False and Misleading Statements in Website Privacy Policies**

Nebraska prohibits knowingly making a false or misleading statement in a privacy policy, published on the Internet or otherwise distributed or published, regarding the use of personal information submitted by members of the public. Pennsylvania includes false and misleading statements in privacy policies published on Websites or otherwise distributed in its deceptive or fraudulent business practices statute.

**Notice of Monitoring of Employee E-mail Communications and Internet Access**

Connecticut and Delaware require employers to give notice to employees prior to monitoring e-mail communications or Internet access.⁶

After Congress rescinded the FCC's privacy rules for internet providers, various states are considering legislation that would restrict how ISPs collect and use consumer data. Nevada and Montana now require ISPs to maintain the privacy of certain customer information absent consent, and California adopted the California Consumer Privacy Act as discussed under Year in Review above. 24 other states are considering their own legislative proposals.

**Children's online privacy**

California prohibits websites directed to minors from advertising products based on information specific to that minor. The law also requires the website operator to permit a minor to request removal of content or information posted on the operator's site or service by the minor, with certain exceptions.⁷

**IV INTERNATIONAL DATA TRANSFER AND DATA LOCALISATION**

There are no significant or generally applicable data transfer restrictions in the United States; however, the United States has taken steps to provide compliance mechanisms for companies

---

⁷ Calif Bus & Prof Code Sections 22580–22582.
that are subject to data transfer restrictions set forth by other countries. The ruling by the CJEU that the US–EU Safe Harbor Framework is ‘invalid’ has brought a considerable degree of uncertainty to the thousands of companies that rely on it as a bedrock of day-to-day global operations. This development had a significant impact on businesses that rely on Safe Harbor to legitimise transfers of personal data from the EU to the United States.

The EU–US Privacy Shield provides a new framework for transatlantic data transfers. The new agreement, which was announced in February and activated in August, replaces Safe Harbor, which was invalidated by the European Court of Justice in October 2015. The new agreement places more stringent duties on US companies to safeguard Europeans’ personal data and on the US Department of Commerce and the FTC for increased scrutiny, enforcement and partnership with European data protection authorities. As part of the framework, the United States agrees that there will be no indiscriminate mass surveillance and access to data for law enforcement and national security purposes with respect to data transferred under the new framework, and must meet certain checks to ensure data are only accessed as necessary and proportionate. In addition, European citizens who believe their data have been compromised in violation of the new agreement will be able to bring complaints to a dedicated ombudsperson. However, some elements of the new agreement share qualities with the now-defunct Safe Harbor, including that companies will subscribe to data protection principles, and that there will be a structured redress process.

In 2012, the United States was approved as the first formal participant in the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules system, and the FTC became the system’s first privacy enforcement authority. The FTC’s Office of International Affairs works with consumer protection agencies globally to promote cooperation, combat cross-border fraud and develop best practices. In particular, the FTC works extensively with the Global Privacy Enforcement Network and APEC.

V COMPANY POLICIES AND PRACTICES

A recent study of corporate privacy management reveals the success of enforcement in pushing corporate privacy managers to look beyond the letter of the law to develop state-of-the-art privacy practices that anticipate FTC enforcement actions, best practices and other forms of FTC policy guidance. Many corporate privacy managers explain that the constant threat and unpredictability of future enforcement by the FTC and parallel state consumer protection officials, combined with the deterrent effect of enforcement actions against peer companies, motivate their companies to proactively develop privacy policies and practices that exceed industry standards. Other companies respond by hiring a privacy officer, or by creating or expanding a privacy leadership function. The risk of enforcement has also prompted companies to engage in ongoing dialogues with the FTC and state regulators.

---

20 See ‘APEC Overview’, Chapter 2.
Corporate privacy managers have also emphasised that while compliance-oriented laws in other jurisdictions do not always keep pace with technological innovation, the FTC’s Section 5 enforcement authority allows it to remain nimble in protecting consumer privacy as technology and consumer expectations evolve over time.

The United States does not require companies to appoint a data protection officer (although specific laws such as the GLBA and HIPAA require companies to designate employees to be responsible for the organisation’s mandated information security and privacy programmes). However, it is best practice to appoint a chief privacy officer and an IT security officer. Most businesses in the United States are required to take reasonable physical, technical and organisational measures to protect the security of sensitive personal information, such as financial or health information. An incident response plan and vendor controls are not generally required under federal laws (other than under the GLBA and HIPAA), although they are best practice in the United States and may be required under some state laws. Regular employee training regarding data security is also recommended. Under the FCC’s now judicially upheld Open Internet Order, broadband ISPs are now also likely to be expected to have incident response plans and vendor controls for data security.

Some states have enacted laws that impose additional security or privacy requirements. For example, Massachusetts regulations require regulated entities to have a comprehensive, written information security programme and vendor security controls, and California requires covered entities to have an online privacy policy with specific features, such as an effective date. And, on 22 May 2018, Vermont enacted the first state-level measure aimed at data brokers. The law requires data brokers to register as such with the Secretary of State, or be subject to civil and other penalties. It also requires data brokers to disclose information about their collection activities, adopt standard security measures, and notify authorities of security breaches.

VI DISCOVERY AND DISCLOSURE

Companies may be required under various federal and state laws to produce information to law enforcement and regulatory authorities, and to civil litigation demands. For example, companies may be ordered to produce information based on federal or state criminal authorities issuing a search warrant, a grand jury subpoena or a trial subpoena, or federal or state regulatory authorities issuing an administrative subpoena. Further, companies could be ordered to produce information upon receiving a civil subpoena in civil litigation.

Such US legal demands may create potential conflicts with data protection or privacy law outside the United States. Companies should consider these possible conflicts when crafting their global privacy and data protection compliance programmes. Consideration should be given to whether US operations require access to European data, such that European data could be considered within the company’s lawful control in the United States and thereby subject to production requests irrespective of European blocking statutes.

The United States does not have a blocking statute. Domestic authorities generally support compliance with requests for disclosure from outside the jurisdiction. The principle of comity is respected, but national law and the Federal Rules of Civil Procedure typically trump foreign law.22

22 Société Nationale Industrielle Aérospatiale v. US District Court, 482 US 522, 549 (1987) (requiring a detailed comity analysis balancing domestic and foreign sovereign interests, in particular US discovery interests and
In a highly significant recent case, the federal court in the Southern District of New York (Manhattan) ruled that Microsoft could be required to transfer customer communications (the contents of emails) stored in Ireland to law enforcement in the United States.\textsuperscript{23} However, in July 2016, the Second Circuit overturned the District Court’s decision, holding that the government cannot force Microsoft to turn over customer emails stored outside the United States.\textsuperscript{24} The issue in the case concerns whether a search warrant served in the United States could authorise the extraterritorial transfer of customer communications notwithstanding the laws of Ireland and the availability of the mutual legal assistance treaty process. The Second Circuit held that Microsoft would not have to turn over customer emails stored in Ireland because the warrant provision of the Stored Communications Act (SCA) does not extend to data stored on foreign servers. The Court stated that ‘Congress did not intend the SCA’s warrant provisions to apply extraterritorially’. Microsoft’s resistance to the US government’s search warrant was supported by numerous other communications and tech companies. Microsoft hailed this decision as one that ensures people’s privacy rights are protected by the laws of their own country, as well as one that prevents foreign governments from accessing consumer data stored within the United States. On 17 April 2018, the United States Supreme Court vacated and remanded the case, with instructions to dismiss it as moot in light of the 23 March 2018 enactment of the Clarifying Lawful Overseas Use of Data Act (CLOUD Act), and subsequent warrant from the government for the information pursuant to the new law.

In a significant January 2018 case, \textit{Leibovic v. United Shore Fin. Servs., LLC}, the United States Court of Appeals for the Sixth Circuit issued a decision that concluded a company had implicitly waived privilege when it disclosed certain materials relating to a privileged forensic data breach investigation in response to a discovery request.\textsuperscript{25} The Sixth Circuit’s decision emphasises the need for caution by litigants wishing to raise a defence that relies on privileged investigations and reports, including third-party forensic reports, or otherwise disclosing the conclusions of such investigations and reports.

\section*{VII PUBLIC AND PRIVATE ENFORCEMENT}

\subsection*{i Enforcement agencies}

Every business in the United States is subject to privacy laws and regulations at the federal level, and frequently at the state level. These privacy laws and regulations are actively enforced by federal and state authorities, as well as in private litigation. The FTC, the Executive Branch and state attorneys general also issue policy guidance on a number of general and specific privacy topics.

Like many other jurisdictions, the United States does not have a central \textit{de jure} privacy regulator. Instead, a number of authorities – including, principally, the FTC and state

\cite{23}{In re Warrant to Search a Certain Email Account Controlled & Maintained by Microsoft Corp, 15 F Supp 3d 466.}
\cite{24}{In re Warrant to Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp, No. 14-02985 (2nd Cir 14 July 2016).}
\cite{25}{See In re United Shore Fin. Servs., LLC, No. 17-2290, 2018 WL 2283893, at *1 (6th Cir 3 January 2018).}
consumer protection regulators (usually the state attorney general) – exercise broad authority to protect privacy. In this sense, the United States has more than 50 de facto privacy regulators overseeing companies’ information privacy practices. Compliance with the FTC’s guidelines and mandates on privacy issues is not necessarily coterminous with the extent of an entity’s privacy obligations under federal law – a number of other agencies, bureaus and commissions are endowed with substantive privacy enforcement authority.

Oversight of privacy is by no means exclusively the province of the federal government – state attorneys general have increasingly established themselves in this space, often drawing from authorities and mandates similar to those of the FTC. The plaintiff’s bar increasingly exerts its influence, imposing considerable privacy discipline on the conduct of corporations doing business with consumers.

At the federal level, Congress has passed robust laws protecting consumers’ sensitive personal information, including health and financial information, information about children and credit information. At the state level, nearly all 50 states have data breach notification laws on the books, and many state legislatures – notably California – have passed privacy laws that typically affect businesses operating throughout the United States.

**FTC**

The FTC is the most influential government body that enforces privacy and data protection in the United States. It oversees essentially all business conduct in the country affecting interstate (or international) commerce and individual consumers. Through exercise of powers arising out of Section 5 of the FTCA, the FTC has taken a leading role in laying out general privacy principles for the modern economy. Section 5 charges the FTC with prohibiting ‘unfair or deceptive acts or practices in or affecting commerce’. The FTC’s jurisdiction spans across borders – Congress has expressly confirmed the FTC’s authority to provide redress for harm abroad caused by companies within the United States.

Former FTC Commissioner Julie Brill noted, ‘the FTC has become the leading privacy enforcement agency in the United States by using with remarkable ingenuity, the tools at its

---


29 This discussion refers generally to ‘privacy’ even though, typically, the subject matter of an FTC action concerns ‘data protection’ more than privacy. This approach follows the usual vernacular in the United States.


31 See www.ftc.gov/about-ftc/what-we-do.

32 15 USC Section 45.

33 15 USC Section 45(a)(4).
disposal to prosecute an impressive series of enforcement cases’.\textsuperscript{34} Using this authority, the FTC has brought numerous privacy deception and unfairness cases and enforcement actions, including over 100 spam and spyware cases and approximately 60 data security cases.\textsuperscript{35}

The FTC has sought and received various forms of relief for privacy related ‘wrongs’ or bad acts, including injunctive relief, damages and the increasingly popular practice of consent decrees. Such decrees require companies to unequivocally submit to the ongoing oversight of the FTC, and to implement controls, audit, and other privacy enhancing processes during a period that can span decades. These enforcement actions have been characterised as shaping a common law of privacy that guides companies’ privacy practices.\textsuperscript{36}

‘Deception’ and ‘unfairness’ effectively cover the gamut of possible privacy-related actions in the marketplace. Unfairness is understood to encompass unexpected information practices, such as inadequate disclosure or actions that a consumer would find ‘surprising’ in the relevant context. The FTC has taken action against companies for deception when false promises, such as those relating to security procedures that are purportedly in place, have not been honoured or implemented in practice. As part of this new common law of privacy (which has developed quite aggressively in the absence of judicial review), the FTC’s enforcement actions include both online and offline consumer privacy practices across a variety of industries, and often target emerging technologies such as the internet of things.

The agency’s orders generally provide for ongoing monitoring by the FTC, prohibit further violations of the law and subject businesses to substantial financial penalties for order violations. The orders protect all consumers dealing with a business, not just the consumers who complained about the problem. The FTC also has jurisdiction to protect consumers worldwide from practices taking place in the United States – Congress has expressly confirmed the FTC’s authority to redress harm abroad caused from within the United States.\textsuperscript{37}

### The states

Similarly to the FTC, state attorneys general retain powers to prohibit unfair or deceptive trade practices arising from powers granted by ‘unfair or deceptive acts and practices’ statutes. Recent privacy events have seen increased cooperation and coordination in enforcement among state attorneys general, whereby multiple states will jointly pursue actions against companies that experience data breaches or other privacy allegations. Coordinated actions among state attorneys general often exact greater penalties from companies than would typically be obtained by a single enforcement authority. In the past two years, several state attorneys general have formally created units charged with the oversight of privacy, in states such as California, Connecticut and Maryland.

The mini FTCAs in 43 states and the District of Columbia include a broad prohibition against deception that is enforceable by both consumers and a state agency. In 39 states and the District of Columbia, these statutes include prohibitions against unfair or unconscionable acts, enforceable by consumers and a state agency.

\textsuperscript{36} See, for example, Solove and Harzog, 2014 (see footnote 29).
\textsuperscript{37} 15 USC Section 45(a)(4).
Recent enforcement cases

FTC data protection enforcement

The FTC’s data protection enforcement has spanned both privacy and security cases, and has focused on both large and small companies across a variety of industries. Some illustrative cases are summarised below.

Internet of things

The FTC recently broke new ground by bringing an enforcement action in the emerging field of the ‘internet of things’. In September 2013, the FTC announced that it settled a case with TRENDnet, a company that markets video cameras designed to allow consumers to monitor their homes remotely. The FTC’s complaint charged that the company falsely claimed in numerous product descriptions that its cameras were ‘secure’; in reality, the cameras were equipped with faulty software that permitted anyone with the cameras’ internet address to watch or listen online. As a result, hundreds of consumers’ private camera feeds were made public on the internet. The FTC’s order imposes numerous requirements on TRENDnet:

a. a prohibition against misrepresenting the security of its cameras;
b. the establishment of a comprehensive information security programme designed to address security risks;
c. submitting to third-party assessments of its security programmes every two years for the next 20 years;
d. notifying customers of security issues with the cameras and the availability of the software update to correct them; and
e. providing customers with free technical support for the next two years.38

The FTC issued a report on the internet of things, ‘Internet of Things: Privacy & Security in a Connected World’, in 2015. Two years in the making, the report provides recommendations to companies about protecting consumer privacy and securing customer data created by the new world of sensors and wearables – mainly by building security into products and services, minimising data collection, and giving consumers notice and choice about how their data are used. The report considers new statutes to be premature, but does suggest that the agency intends to adapt existing authorities under the FTCA, the FCRA and COPPA. Republican Commissioner Wright dissented from the report, arguing that the FTC should not issue recommendations and best practices without engaging in a cost–benefit analysis to determine that such measures would, if adopted, improve consumer welfare. Commissioner Wright also suggested that the Commission departed from standard practice by issuing policy recommendations in a workshop report, as such reports typically serve only to ‘synthesize the record developed during the proceedings’. Addressing attendees at the Better Business 2016 Conference in Washington, DC on 21 April 2016, Federal Trade Commissioner Maureen Ohlhausen remarked that the Commission should examine existing privacy regulations to determine how they apply to the potential new privacy risks created by the internet of things.

Commissioner Ohlhausen expressed excitement about the potential benefits that smart devices can bring, but cautioned that these technologies carry with them new risks with respect to data collection and surveillance.

In 2016, the FTC published another report, entitled ‘Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues’. The report focused on how Big Data are used after being collected and analysed, and presented questions for businesses to consider to avoid exclusionary or discriminatory outcomes for consumers. The report discussed innovative uses of Big Data that are benefiting underserved populations, such as through increased educational and healthcare opportunities, but also looked at risks that could arise from biases about certain groups. The report discusses numerous factors for companies to consider to enhance the relevance, quality, accuracy, objectivity and fairness of predictions and decision-making based on Big-Data analytics and embedded algorithms.

On 8 January 2018, the FTC announced a settlement with VTech (a maker of electronic children’s toys) for violations of COPPA, adding to the regulatory activity mounting in the last few years around the internet of things, and more specifically, the internet of toys. The company agreed to pay US$650,000 to settle allegations that its app and platform collected personal information from almost 3,000,000 children without providing direct notice and obtaining their parent or guardian’s consent. Specifically, the FTC alleged that the company failed to provide a link to its privacy policy in each area where personal information was collected from children. The FTC also alleged that the company failed to take reasonable steps to secure the data it collected in violation of both COPPA and the FTC Act, and that these poor data security practices contributed to a November 2015 data breach.

Financial and medical information

The SEC Office of Compliance Inspections and Examinations (OCIE) issued guidance on cybersecurity and announced examination priorities, taking multiple steps to heighten its enforcement presence for cybersecurity matters and identifying cybersecurity as an SEC OCIE exam priority for 2018. The SEC took several cybersecurity-related steps in September 2015 that related to its mandate to oversee investment advisers and broker-dealers, and to protect investors. OCIE issued a risk alert setting forth concrete guidance for broker-dealers and investment advisers, including notably a view that multifactor authentication was a ‘basic control’. The alert served to announce cybersecurity as a renewed area of focus for examinations, and included a sample document request for upcoming exams. Further, the SEC announced that it reached a settlement with R T Jones, an investment adviser that did not have cybersecurity policies and procedures in place prior to a breach. Despite the company’s immediate remedial steps, the SEC found that R T Jones’s failure to maintain such policies was a violation of Regulation S-P. In connection with the settlement, the Office of Investor Education and Advocacy announced an investor alert to heighten individual awareness regarding response to identity theft or data breaches impacting their investment accounts. In August 2017, OCIE issued a summary of observations from recent sweep exams of broker-dealers, investment advisers and funds. OCIE reported an improvement in awareness of cyber risks and implementation of cybersecurity practices in the past few years. Nearly all entities examined maintained written cybersecurity policies and procedures. OCIE noted, however, that many policies were not sufficiently detailed and were overly vague, and recommended that policies should be ‘reasonably tailored’ to the company. There were also noted issues with companies failing to follow their written policies, follow up with remediation when issues were discovered or patch systems appropriately. In 2018, the SEC
issued new guidance on cybersecurity disclosures in SEC filings. In addition to information on cybersecurity disclosure controls and procedures, the guidance included components on policies to prevent insider trading based on non-public cyber information.

**Mini FTCA privacy enforcement cases**

In the past few years, state attorneys general have brought a number of enforcement actions pursuant to their authority under their respective states’ mini FTCAs. Two illustrative examples are summarised below.

**Google Street View settlement**

In 2013, 38 state attorneys general reached a US$7 million settlement with Google over allegations that the company violated people’s privacy by collecting Wi-Fi data as part of its Street View activities. Google agreed to train its employees about privacy and confidentiality for at least the next 10 years, and to destroy or secure any improperly collected information.39

**Safari cookie settlements**

In 2013, 37 states settled, for US$17 million, an investigation with Google involving allegations that the company bypassed web browser privacy settings to collect consumers’ browsing information. Another settlement related to this incident, which was already approved by a judge and requires Google to donate more than US$3 million to schools and non-profits, is now being criticised by attorneys general from 11 states, who argue that the settlement should provide for the money to go to the people who were allegedly affected.

**Robocalls**

The FCC remains interested in preventing robocalls. The FCC issued its biannual warning to political campaigns about robocalls and text abuse in March 2016. The FCC’s warning said the FCC ‘is committed to protecting consumers from harassing, intrusive, and unwanted robocalls and texts, including to cell phones and other mobile devices’. The warning pledged that the FCC’s Enforcement Bureau will ‘rigorously enforce’ the TCPA. On 16 March 2018, the US Court of Appeals for the DC Circuit issued a ruling on a challenge to the FCC’s 2015 order that expanded the scope of the Telephone Consumer Protection Act (TCPA). In *ACA International v. FCC*, the court invalidated a rule that had broadly defined automatic telephone dialing systems, or ‘auto-dialers’; it also struck down the FCC’s approach to situations where a caller obtains a party’s consent to be called but then, unbeknownst to the caller, the consenting party’s wireless number is reassigned.40 In the same ruling, the court upheld the FCC’s decision to allow parties who have consented to be called to revoke their consent in ‘any reasonable way,’ as well as the FCC’s decision to limit the scope of an exemption to the TCPA’s consent requirement for certain healthcare-related calls. Following the ruling, the FCC issued a public notice seeking input about how it should interpret the TCPA.

---


Unsolicited faxes

The FCC imposed a US$1.84 million penalty against Scott Malcolm, DSM Supply and Somaticare for sending 115 unsolicited fax advertisements to the fax machines of 26 consumers. The faxes were primarily sent to healthcare practitioners. The FCC issued this forfeiture order in February 2016.

iii Private litigation

Privacy rights have long been recognised and protected by common law. The legal scholar William Prosser created a taxonomy of four privacy torts in his 1960 article ‘Privacy’ and later codified the same in the American Law Institute’s Restatement (Second) of Torts. The four actions for which an aggrieved party can bring a civil suit are:

- intrusion upon seclusion or solitude, or into private affairs;
- public disclosure of embarrassing private facts;
- publicity that places a person in a false light in the public eye; and
- appropriation of one’s name or likeness.

These rights protect not only the potential abuse of information, but generally govern its collection and use.

The plaintiff’s bar

The plaintiff’s bar is highly incentivised to vindicate commercial privacy rights through consumer class action litigation. The wave of lawsuits that a company faces after being accused in the media of misusing consumer data, being victimised by a hacker or suffering a data breach incident is well known across the country. A plaintiff’s litigation around the Video Privacy Protection Act (VPPA) may attempt to take advantage of a narrow opening in the First Circuit, which broadens the statute’s definition of personally identifiable information to find liability against companies that disclose information about consumers’ video viewing. In In re Nickelodeon Consumer Privacy Litigation, the Third Circuit held that ‘personally identifiable information under the Video Privacy Protection Act means the kind of information that would readily permit an ordinary person to identify a specific individual’s video-watching behavior’. This narrow definition of personally identifiable information is upheld across numerous jurisdictions. However, this creates a circuit split with the First Circuit, which held in Yershov v. Gannett Satellite Information Network Inc that the VPPA was violated when a company disclosed a unique anonymous Adobe ID, GPS coordinates and video title information without consent to a third party.

Role of courts

Courts remain central to defining and reshaping the contours of privacy rights and remedies. This role goes beyond the role of trial courts in adjudicating claims brought by regulators and private parties that seek to protect and define privacy rights and remedies; interest in these issues has been expressed at the highest levels. The Supreme Court has demonstrated recent interest on commercial privacy matters. Although it refused to take up Spokeo, Inc v. Robins again in 2018, in 2016, the Supreme Court held that an injury suffered under the

---

41 827 F.3d 262, 290 (3d Cir 27 June 2016).
42 820 F3d 482, 489-90 (1st Cir 29 April 2016).
FCRA must be sufficiently ‘concrete’ to find standing (discussed above). The Court held that a bare procedural violation was insufficient for proper standing. Additionally, in a November 2013 dismissal of a petition for certiorari, Chief Justice Roberts noted in dicta what issues the Court might consider when evaluating the fairness of class action remedies brought by plaintiffs challenging a privacy settlement.\(^4\) Consumer protection regulators like the FTC and state attorneys general are becoming increasingly aggressive, both in terms of the scope of enforcement jurisdiction and the stringency of regulator expectations.

**VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS**

Foreign organisations can face a federal or state regulatory action or private action if the organisation satisfies normal jurisdictional requirements under US law. Jurisdiction typically requires minimum contacts with or presence in the United States. Additionally, a foreign organisation could be subject to sector-specific laws if the organisation satisfies that law’s trigger. For example, if a foreign organisation engages in interstate commerce in the United States, the FTC has jurisdiction. If a foreign organisation is a publicly traded company, the SEC has jurisdiction. If an organisation is a healthcare provider, the Department of Health and Human Services has jurisdiction.

Additionally, foreign organisations must consider the residency of their data subjects. Massachusetts information security regulations apply whenever an organisation processes data of Massachusetts residents. Since Massachusetts was among the first states to enact highly detailed information security requirements, its rules have become a de facto consideration for national best practices.

The United States does not have a general data localisation requirement, although certain requirements do exist for government contractors. Although the United States does generally require data localisation, it requires vendor oversight to ensure reasonable standards of data care. Foreign organisations operating in the United States should know that they are the responsible party under US law even if data processing is handled by a vendor outside the United States.

The United States does not have any jurisdictional issues for multinational organisations related to cloud computing, human resources and internal investigations. However, foreign organisations subject to US law should carefully consider how their data network is structured, and ensure they can efficiently respond to international data transfer needs, including for legal process. The United States respects comity, but a foreign country’s blocking statute does not trump a US legal requirement to produce information.

**IX CYBERSECURITY AND DATA BREACHES**

Cybersecurity has been the focus of intense attention in the United States in recent years, and the legal landscape is dynamic and rapidly evolving. Public discourse has tended to conflate distinct legal issues into a single conversation that falls under the blanket term ‘cybersecurity’. Cybersecurity law and policy are more accurately described and characterised

in distinct buckets: primarily consumer or personal information on the one hand, and critical infrastructure or sensitive corporate data on the other. Of course, the same or similar safeguards provide protection in both contexts.

While the United States does not have an omnibus law that governs data security, an overlapping and comprehensive set of laws enforced by federal and state agencies provides for the security of this information. These information security safeguards for personal and consumer information, as well as data breach notification provisions, are prescribed in the federal GLBA (financial data), HIPAA (healthcare data) and 50 state laws, plus the laws of numerous US territories and districts such as the District of Columbia (for broad categories of sensitive personal information). The GLBA, HIPAA and Massachusetts state law\(^44\) provide the most detailed and rigorous information security safeguards. The emergence of the National Institute for Standards and Technology (NIST) cybersecurity framework, as detailed below, is likely to emerge as the predominant framework under which companies undertake to ensure information security.

Fifty states and various US jurisdictions have enacted data breach notification laws, which have varying notification thresholds and requirements. These laws generally require that individuals be notified, usually by mail (although alternate notice provisions exist), of incidents in which their personal information has been compromised. These laws usually include a notification trigger involving the compromise of the name of an individual and a second, sensitive data element such as date of birth or credit card account number.

The GLBA Safeguards Rule requires financial institutions to protect the security and confidentiality of their customers’ personal information, such as names, addresses, phone numbers, bank and credit card account numbers, income and credit histories, and social security numbers. The Safeguards Rule requires companies to develop a written information security plan that is appropriate to the company’s size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles. As part of its plan, each company must:

\(\begin{align*}
a & \text{ designate an employee to coordinate its information security programme;} \\
b & \text{ conduct a risk assessment for risks to customer information in each relevant area of the company’s operation and evaluate the effectiveness of the current safeguards for controlling these risks;} \\
c & \text{ design and implement a safeguards programme, and regularly monitor and test it;} \\
d & \text{ select service providers that can maintain appropriate safeguards, contractually require them to maintain such safeguards and oversee their handling of customer information;} \\
e & \text{ evaluate and adjust the programme in light of relevant circumstances, including changes in the firm’s business or operations, or the results of security testing and monitoring.}\(^45\)
\end{align*}\)

The SEC has broad investigative and enforcement powers over public companies that have issued securities that are subject to the Securities Acts, and enforce this authority through the use of a number of statutes, including Sarbanes-Oxley. The SEC has investigated companies that are public issuers that have suffered cybersecurity incidents, including Target, and has


considered theories, including that material risks were not appropriately disclosed and reported pursuant to the agency’s guidance on how and when to disclose material cybersecurity risk; and that internal controls for financial reporting relating to information security did not adequately capture and reflect the potential risk posed to the accuracy of financial results. The SEC also enforces Regulation S-P, which implements the privacy and security provisions of the GLBA for entities subject to its direct regulatory jurisdiction (such as broker-dealers and investment advisers). In 2015, the SEC and its ‘self-regulatory’ counterpart, the Financial Industry Regulatory Authority, issued guidance and ‘sweep’ reports regarding the state of data security among broker-dealers and investment advisers.

On 21 February 2018, the SEC published new interpretive guidance to assist publicly traded companies in disclosing their material cybersecurity risks and incidents to investors. The SEC suggested that all public companies adopt cyber disclosure controls and procedures that enable companies to:

a. identify cybersecurity risks and incidents;
b. assess and analyse their impact on a company’s business;
c. evaluate the significance associated with such risks and incidents;
d. provide for open communications between technical experts and disclosure advisers;
e. make timely disclosures regarding such risks and incidents; and,
f. adopt internal policies to prevent insider trading while the company is investigating a suspected data breach.

The Department of Health and Human Services administers the HIPAA Breach Notification Rule, which imposes significant reporting requirements and provides for civil and criminal penalties for the compromise of PHI maintained by entities covered by the statute (covered entities) and their business associates. The HIPAA Security Rule also requires covered entities to maintain appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity and security of electronic PHI.

In April 2015, the Department of Justice issued its own guide, Best Practices for Victim Response and Reporting of Cyber Incidents. The Department noted concerns about working with law enforcement after suffering a data breach: ‘Historically, some companies have been reticent to contact law enforcement following a cyber incident fearing that a criminal investigation may result in disruption of its business or reputational harm. However, a company harbouring such concerns should not hesitate to contact law enforcement.’

Several states also require companies operating within that state to adhere to information security standards. The most detailed and strict of these laws is the Massachusetts Data Security Regulation, which requires that companies maintain a written information security policy (commonly known as a WISP) that covers technical, administrative and physical controls for the collection of personal information.

In February 2013, President Obama issued Executive Order 13,636, ‘Improving Critical Infrastructure Cybersecurity’. This Executive Order directs the Department of Homeland Security to address cybersecurity and minimise risk in the 16 critical infrastructure sectors identified pursuant to Presidential Policy Directive 21. The Order directed the NIST to develop a cybersecurity framework, the first draft of which was released in February 2014.

47 Available at www.dhs.gov/critical-infrastructure-sectors.
The NIST Cybersecurity Framework provides voluntary guidance to help organisations manage cybersecurity risks, and ‘provides a means of expressing cybersecurity requirements to business partners and customers and help identify gaps in an organisation’s cybersecurity practices’. While the framework is voluntary and aimed at critical infrastructure, there is an increasing expectation that use of the framework (which is laudably accessible and adaptable) could become a best practice consideration for companies holding sensitive consumer or business proprietary data. Companies operating in highly regulated industries such as the defence industrial base, energy sector, healthcare providers, banks subject to detailed examinations by the Federal Financial Institutions Examination Council and investment firms that are regulated by the SEC are subject to detailed cybersecurity standards.

Congress cybersecurity legislation in December 2015, known as the Cybersecurity Act. This law includes CISA, which is designed to foster cyberthreat information sharing and provided certain liability shields related to such sharing and other cyber-preparedness. Specifically, CISA provides liability protection for sharing cyberthreat information with government and private parties. CISA also authorises network monitoring and other defensive measures, notwithstanding any other provision of law.

On 11 May 2017, the White House followed up on the 2016 PPD-41 with a cybersecurity executive order that requires further studies and outlines priorities for the current administration’s cybersecurity efforts. The executive order calls for an assessment of critical infrastructure and seeks to build the government’s cybersecurity capacities by updating old technologies and hiring more skilled technologists. It also strongly endorsed the NIST Cybersecurity Framework, requiring all agencies to use the NIST Cybersecurity Framework to manage cyberrisks. On 16 August 2017, NIST issued an updated draft of its security and privacy guidance for federal information systems, providing specific guidance on internet-of-things (IOT) devices and on how to apply this guidance outside the government sector. NIST finalised the guidance and released an updated version of its Cybersecurity Framework on 17 April 2018.

As detailed above, the FTC also increasingly plays the role of de facto cybersecurity enforcement agency where consumers or personal information are involved. Based on Section 5 of the FTCA, the Commission has stated that providing reasonable and appropriate information security is required as a ‘fair’ trade practice. State attorneys general, pursuant to state-level mini FTCAs (see Sections VII.i and ii), have taken a similar approach. Essentially, every major data breach is investigated by the FTC and state attorneys general, and may also draw the attention of other regulators such as the SEC. New York’s Department of Financial Services (DFS) issued a proposed rule in September, which would require banks, insurance companies and other financial service institutions regulated by New York’s DFS to create and maintain a cybersecurity programme designed to protect consumers and New York’s financial industry. The New York DFS rule went into full effect on 28 August 2017, requiring that all financial institutions regulated by DFS create a cybersecurity programme that is approved by the board or a senior corporate official, appoint a chief information security officer, limit access to non-public data, and implement guidelines to notify state regulators of cybersecurity or data security incidents within 72 hours.

Cybersecurity remains a headline issue. In September and December 2016, Yahoo! announced that data associated with at least 500 million user accounts were stolen by what was later confirmed to be a state-sponsored actor. In December 2016, Yahoo! announced a second breach affecting 1 billion users that dated back to 2013. These two incidents are considered as possibly the largest cybersecurity breaches ever reported. The FBI announced
on 11 August 2016 that it is nearly certain that the hacking of the Democratic Party in late July was the work of the Russian government. The federal investigation of the hack revealed that, in addition to the DNC and to the Democratic Congressional Campaign Committee, other party-affiliated groups were targeted in the hack, which probably included the breach of personal email accounts of the groups and group leaders. On 20 March 2017, after the 2016 election and inauguration of President Donald Trump, the FBI confirmed that it was investigating the Russian government’s interference in the 2016 election. In September 2017, the consumer reporting agency Equifax announced that the sensitive financial information of 143 million Americans had been exposed to hackers that exploited an unpatched website vulnerability. Given the pivotal role of credit bureaus such as Equifax, the ramifications of this breach may impact decision-making in the consumer financial sector.

In 2018, Yahoo! settled cybersecurity allegations brought by the SEC (for US$35 million) and by shareholders for (US$80 million).

X OUTLOOK

With regard to privacy regulation of internet, telecom and tech companies, it is still not certain in which direction new regulators appointed by the Trump administration will head. Privacy has not been an especially partisan issue in the United States to date.

Under new FTC Chairman Joseph Simons, the agency ‘will hold a series of public hearings during the fall and winter 2018 examining whether broad-based changes in the economy, evolving business practices, new technologies, or international developments might require adjustments to competition and consumer protection law, enforcement priorities, and policy.’ These hearings will include coverage of privacy and cybersecurity enforcement. Public comments have been solicited on the FTC’s authority to deter unfair and deceptive conduct in privacy and data security matters, including the identification of any additional tools or authorities necessary to adequately deter unfair and deceptive conduct related to privacy and data security.

There are also indications that the White House is considering the development of a new privacy framework that may be published by a component of the Department of Commerce in the fall of 2018.
ABOUT THE AUTHORS

DIEGO ACOSTA-CHIN
Santamarina y Steta, SC

Mr Acosta-Chin obtained his law degree from the Monterrey Institute of Technology and Higher Education in 2008. He is fluent in Spanish and English.

Mr Acosta-Chin joined Santamarina y Steta, SC in 2009, and since then his professional practice has been focused on corporate matters, including mergers and acquisitions, data privacy matters, the prevention of money laundering, e-commerce and foreign investment.

Mr Acosta-Chin’s practice focuses on data privacy matters, and he advises clients on analyses of the implications of, and actions necessary for compliance with, data privacy legislation, including the drafting and filing of writs with respect to official communications issued by the National Institute of Transparency, Access to Information and Protection of Personal Data regarding its surveillance and enforcement divisions, mapping of the processing of personal data throughout different departments or business units of an organisation, drafting the required documents to comply with the law, coordinating efforts to be in compliance with the law, advising on breaches of personal data confidentiality obligations and implementing cross-border contingency plans to mitigate and prevent security breaches, among other matters.

KAAN CAN AKDERE
BTS&Partners

Kaan Can Akdere graduated from Koç University, faculty of law in 2016 and achieved his master’s degree from the University of Edinburgh in 2017. Kaan focuses on Turkish personal data protection law and regulatory compliance matters with regard to information and communications technologies. He advises both local and international clients on matters such as data protection, cybersecurity, e-commerce, digital advertising and telecommunication law. He is a member of European Law Students Association’s Turkish branch and is admitted to the Istanbul Bar Association.

MERCEDES DE ARTAZA
M&M Bomchil

Mercedes de Artaza is a senior lawyer in the competition and antitrust, foreign trade, and mergers and acquisitions departments. She joined the firm in 2011.
She graduated as a lawyer from the Catholic University and completed her masters’ degree in corporate law at the Austral University. She is also a professor of company law in the University of Buenos Aires since 2007.

Her practice focuses on providing advice on anticompetitive and anti-dumping investigations, foreign trade and import-export regimes, the defence of merger, acquisition and joint venture operations before the competition authorities, compliance, data protection, anticorruption laws, and advice on corporate and contractual matters. She has represented important local and foreign companies in matters relating to her area of expertise.

She is the author of several publications on issues linked to her areas of specialisation and a speaker at conferences in Argentina and abroad.

Her professional performance has been recognised by various specialised publications, including Chambers Latin America and Best Lawyers.

NATALIA BARRERA SILVA
Marquez, Barrera, Castaneda & Ramirez

Natalia Barrera Silva is a law graduate of Pontificia Universidad Javeriana and holds an LLM degree from Columbia University, where she attended as a Fulbright scholar. She also holds a specialisation certificate in competition and free trade law from Pontificia Universidad Javeriana and a specialisation certificate in regulation of telecommunications and new technologies from Universidad Externado de Colombia.

Mrs Barrera Silva worked as an in-house attorney at Caracol Radio and at the firm Esguerra Barrera Arriaga Abogados, first as an associate in the competition law area and afterwards as director of media, entertainment and technologies. During her master’s studies she interned at Volunteer Lawyers for the Arts in New York.

Mrs Barrera Silva has been assistant lecturer of the competition law course at Pontificia Universidad Javeriana and of the international business law course at Centro de Estudios Superiores de Administracion.

She is fluent in Spanish, English and French and is admitted to practise in Colombia and the state of New York (2011).

REYES BERMEJO BOSCH
Uria Menendez Abogados, SLP

Reyes Bermejo is a lawyer in the Madrid office of Uría Menéndez. She became a lawyer in 2006 and joined the firm in 2011.

She focuses her practice on data protection, e-commerce and IT. Reyes provides national and multinational companies with day-to-day advice in the above-mentioned areas, on matters such as privacy, consumer protection and e-commerce, and dealings with public authorities, including the drafting and negotiation of IT agreements. In particular, she has extensive experience in the data protection design of commercial and M&A transactions, in the preparation of notices, clauses, contracts, protocols and training programmes, in authorisation proceedings for international transfers and administrative and judicial proceedings, and in preparing website terms and conditions and cookie policies and in advising on direct marketing activities by electronic means.

Reyes is also a professor of data protection and e-commerce law on various master’s degree programmes and seminars (the University of Valencia, and the Financial and Stock Market Studies Foundation and CEU Cardenal Herrera University, both also in Valencia).
She contributes to the firm's data protection newsletter and legal magazine (Actualidad Jurídica Uria Menéndez) on aspects of and updates relating to data protection regulatory issues and case law.

FRANCESCA BLYTHE
Sidley Austin LLP
Francesca Blythe is an associate in the London office at Sidley Austin LLP, whose main practice areas are data protection, privacy, cybersecurity, e-commerce and information technology.

ANNE-MARIE BOHAN
Matheson
Anne-Marie Bohan is a partner in both the asset management and investment funds group and the FinTech group at Matheson, and is head of the outsourcing group. She advises on all aspects of outsourcing, information technology law and e-commerce law, with specific focus on the requirements of financial institutions and financial services providers in these areas.

Anne-Marie has extensive experience in drafting and negotiating contracts for the development, sale, purchase and licensing of hardware, software and IT systems for both suppliers and users of IT within the financial services industry and across a broad range of other industries. She has also acted in some of the largest value and most complex IT and telecommunications systems and services outsourcing contracts, including advising on the largest and highest value financial services outsourcing to date, in Ireland. Anne-Marie's practice also includes advising a broad range of clients on data protection and privacy issues, including employee data protection issues.

Anne-Marie has written numerous articles on electronic commerce, internet, security issues, data protection and copyright law, and contributed the Ireland chapter to Outsourcing Contracts – a Practical Guide in 2009. She has also spoken at conferences on IT and electronic commerce issues, including electronic signatures, internet security, e-commerce and data protection. She also contributed the Irish chapter to Getting the Deal Through: e-Commerce in both 2002 and 2003, and has lectured as part of the Law Society of Ireland, diploma in electronic commerce. Anne-Marie was a member of the Matheson team that advised the Department of Public Enterprise on the drafting of the Electronic Commerce Act 2000.

SHAUN BROWN
nNovation LLP
Shaun Brown is a partner with nNovation LLP, an Ottawa-based law firm that specialises in regulatory matters. With several years of experience both in the public and private sectors, Shaun’s practice focuses on e-commerce, e-marketing, privacy, access to information and information security. Shaun assists clients by developing practical and effective risk-mitigation strategies, and by representing clients before tribunals and in litigation-related matters. Shaun has a deep understanding of the online marketing industry from both a technical and legal perspective. He speaks and writes regularly on privacy, marketing and information management issues, is a co-author of The Law of Privacy in Canada, and teaches the same subject in the faculty of law at the University of Ottawa.
ELLYCE R COOPER
Sidley Austin LLP

Ellyce Cooper is a partner in the firm’s Century City office and a member of the complex commercial litigation and privacy and cybersecurity practices. Ellyce has extensive experience in handling government enforcement matters and internal investigations as well as complex civil litigation. She assists companies facing significant investigations and assesses issues to determine a strategy going forward. Ellyce’s diverse experience includes representing clients in internal investigations and government investigations along with responding to and coordinating crisis situations. Her client list includes notable companies from the healthcare, pharmaceutical, accounting, financial, defence and automotive industries. Ellyce earned her JD from the University of California, Los Angeles School of Law and her BA, magna cum laude, from the University of California Berkeley.

CÉSAR G CRUZ-AYALA
Santamarina y Steta, SC

Mr Cruz-Ayala obtained his law degree from the Facultad Libre de Derecho de Monterrey in May 1994, which was followed by a master’s in comparative jurisprudence at New York University School of Law in May 1998. He is fluent in Spanish and English.

Mr Cruz-Ayala joined Santamarina y Steta, SC in 1993 and became a partner in 2006. During that time, his professional practice has been focused on mergers and acquisitions, data privacy matters, prevention of money laundering, and e-commerce, real estate and transnational business projects.

Mr Cruz-Ayala’s practice focuses on data privacy matters and he has a broad knowledge of data privacy legislation and its implications. He advises clients on assessing and complying with Mexican data privacy laws, including mapping of the processing of personal data throughout different departments or business units of an organisation, drafting the documents required to comply with the law, coordinating efforts to be in compliance with the law, advising on breaches of personal data confidentiality obligations and implementing cross-border contingency plans to mitigate and prevent security breaches, among other matters. Mr Cruz-Ayala is very active in the industry and regularly organises and participates in seminars, webinars and conferences in this area.

SANUJ DAS
Subramaniam & Associates

Sanuj specialises in litigation, both IP and non-IP, and is a member of the Subramaniam & Associates litigation team. He also handles patent revocation proceedings before the appellate board, along with patent, trademark and design opposition proceedings. He has worked with a diverse array of clients, including professionals and scientists from the telecommunication, pharmaceutical, FMCG and apparels sectors. In addition to a bachelor’s degree in law, Sanuj holds a bachelor’s and a master’s degree in pharmacy, with a specialisation in pharmaceuticals.
MARISSA (XIAO) DONG

Jun He LLP

Ms Dong is a partner in the Beijing office, specialising in the areas of foreign direct investment, mergers and acquisitions, and data protection, information and cybersecurity law. She represents Fortune 500 corporations and other global enterprises, and Chinese state-owned and private companies, as well as financial services firms, including private equity firms.

In her corporate law practice, Ms Dong guides inbound investors through all stages of operating in China, from market investigation to market entry and business expansion (including incorporating PRC entities and mergers and acquisitions). In addition, she represents prominent Chinese companies in outbound direct investments. Her clients include industry leaders in education, manufacturing and internet and telecommunications services.

She also advises clients on all aspects of data protection, information and cybersecurity law, with a special emphasis on information privacy (consumers, employees and patients), data security and breaches, and international data transfers. Ms Dong helps clients navigate China’s complex and sector-specific policy and regulatory landscape. Her clients include national and international information technology vendors, internet service providers, data brokers, retailers and distributors, and manufacturers of medical, industrial and consumer products.

ADRIÁN LUCIO FURMAN

M&M Bomchil

Adrián Furman is a partner in the mergers and acquisitions and entertainment law departments and in charge of M&M Bomchil’s intellectual property area. He joined the firm in 2000.

He graduated as a lawyer from the University of Buenos Aires in 1998. He obtained a postgraduate degree in corporate business law at the same institution, where he is also a professor of civil and commercial contracts.

He has worked on numerous cross-border transactions and regularly advises corporate clients on various issues of a contractual nature. He also has wide experience of issues of commercial fair trade and consumer protection.

During 2005 he was international associate at the New York offices of Simpson Thacher & Bartlett.

He is a frequent speaker at chambers of commerce on his areas of expertise and at the Section of International Law of the American Bar Association seasonal meetings.

He has been and is a director and auditor of important companies such as PepsiCo, AMC Networks, Telefe and Mindray, among others.

He is co-chair of the International Commercial Transactions, Distribution and Franchise Committee of the Section of International Law of the American Bar Association.

His professional performance has been recognised by various specialised publications, including Chambers Latin America and Best Lawyers, and by the Latin American Corporate Counsel Association and Client Choice Awards.

TAMÁS GÖDÖLLE

Bogsch & Partners Law Firm

Tamás Gödölle graduated from the law faculty of Eötvös Loránd University in Budapest. He studied commercial and international private law for one year at the Ludwig Maximilian
University of Munich in Germany and continued with postgraduate legal studies at Queen Mary and Westfield College, University of London (1990–1991). As a corporate, commercial and intellectual property lawyer, he has been practising in Hungary, advising and representing national and multinational clients, for over 24 years. Dr Gödölle has been a partner at Bogsch & Partners since 1996, where he specialises in trademark, copyright, antitrust, unfair competition and advertising matters, as well as franchise, distributor and licence contracts. He also has extensive experience in information technology, privacy, data protection and life science and media law issues. He is a member of the Budapest Bar, the Hungarian Association for the Protection of Industrial Property and Copyright (MIE), both the Hungarian and the International League of Competition Law (LIDC), ECTA, INTA, AIPPI, ITechLaw and GRUR. As well as speaking Hungarian, he is fluent in English and German.

TOMOKI ISHIARA

Sidley Austin Nishikawa Foreign Law Joint Enterprise

Mr Ishiara’s practice areas include intellectual property law, antitrust law, data security and privacy law, entertainment law, investigation, litigation and arbitration. Mr. Ishiara has extensive experience in the field of intellectual property law, including giving advice to clients on patent, utility model, design patent, copyright, and trademark matters (including advice on employee invention rules), engaging in litigations and arbitrations. Also, Mr. Ishiara regularly advises foreign clients on compliance matters (e.g., data privacy, FCPA) and engages in subsequent investigations on such violations.

SHANTHI KANDIAH

SK Chambers

Shanthi Kandiah founded SK Chambers with the goal of creating a stand-alone regulatory firm that services individuals and entities involved at all levels of the regulatory scheme. Today, SK Chambers does just that – it is focused on delivering legal services in competition law, the full spectrum of multimedia laws, privacy and data protection matters, and anti-bribery and corruption laws, as well as capital market laws and exchange rules.

Shanthi Kandiah regularly advises many corporations in sectors such as media and telecommunications, FMCG, construction and credit reporting on privacy and data protection matters, including the following: compliance strategies that prevent and limit risk; managing risks through contracts with customers and suppliers; data protection and cyberrisk due diligence in relation to acquisitions, dispositions and third-party agreements; crisis management when a data breach occurs; investigations management – when faced with regulatory action for data security breaches; and data transfers abroad – advising on risks and issues.

She holds an LLM and a postgraduate diploma in economics for competition law, both from King’s College London.

MAJA KARCZEWSKA

Kobylanska & Lewoszewski Kancelaria Prawna Sp. J

Maja Karczewska is a lawyer working for Kobylanska & Lewoszewski law firm. Her main fields of interest include media and advertising law, as well as intellectual property law (especially copyright). She also provides legal assistance in the field of personal data protection. Maja
Karczewska regularly publishes articles on personal data protection and intellectual property issues. On day-to-day basis she supports clients from media and new technologies sectors.

**VYACHESLAV KHAYRYUZOV**

*Noerr*

Vyacheslav Khayryuzov heads digital business and data privacy and co-heads the IP practice groups in the Moscow office of Noerr. He advises clients that predominantly operate in the technology, retail, media sectors. His extensive experience includes international copyright and software law, data privacy protection, as well as commercial and media law issues in Russia. In addition, he advises clients on general IP matters. He represents both national and international clients, ranging from start-ups to large national and international corporations.

Vyacheslav joined Noerr in 2007, having previously worked as a senior counsel at Rambler, a major Russian internet company, where he worked on a number of international projects.

He is currently a local representative for Russia in the International Technology Law Association (ITechLaw) and a member of Digitalisation committee of the German–Russian Chamber of Commerce.

Vyacheslav has been recommended for Intellectual Property and TMT by *The Legal 500 EMEA, Chambers Europe, Best Lawyers, Who’s Who Legal* and others.

**BATU KİNİKOĞLU**

*BTS&Partners*

Batu Kınıkoğlu (LLM) is the head of the data protection practice at BTS & Partners. Batu graduated from Istanbul University, Faculty of Law and achieved his masters degree from the University of Edinburgh. He has a broad range of experience on data protection and telecommunications law and is valued by clients for his technical knowledge and dedication. He advises clients on a wide range of issues, including data protection, information privacy, cybersecurity, e-commerce and telecommunications law. His expertise also includes copyright and open source software licensing. He also advises clients on public procurement projects relating to information and communication technologies and has articles published in international academic journals on subjects ranging from copyright to internet regulation.

**ANNA KOBYLAŃSKA**

*Kobylańska & Lewoszewski Kancelaria Prawna Sp J*

Anna Kobylańska, an advocate with 15 years of experience, was in charge of data protection, new technologies and intellectual property in a global advisory company before joining Kobylańska & Lewoszewski as a founding partner. Anna specialises in providing advice on the protection of personal data to clients from the pharmaceuticals, financial services, media and automotive sectors. She regularly oversees projects focused on the analysis and implementation of the provisions of the GDPR. Anna co-authored the book *Protecting Personal Data in the Practice of Entrepreneurs*. She is also a lecturer at the H Grocjusz Centre for Intellectual Property Law, in the field of personal data protection. She was a member of the INTA Committee for the Protection of Personal Data (an international association of trademark law specialists). For the past six years, Anna has been recognised by *Chambers Europe* as one of leading lawyers in Poland in the TMT/data protection category. In 2017, her
practice was recognised by Polish legal ranking company Polityka Insight as one of Poland's foremost teams in the field of personal data.

**FABIO FERREIRA KUJAWSKI**  
*Mattos Filho, Veiga Filho, Marrey Jr e Quiroga Advogados*

Fabio Kujawski is a partner of Mattos Filho, who practises in the telecoms, intellectual property, technology and data privacy fields. Fabio advises companies on a wide range of corporate matters, domestic and cross-border. Fabio is recognised by leading legal directories such as *Chambers and Partners*, *The Legal 500*, *Leaders’ League*, *Latin Lawyer*, *LACCA*, *IFRL1000*, *Who’s Who Legal* and *Euromoney* as a leading practitioner in the areas of data protection, technology and telecommunications. He is the co-author and editor of the book *Legal Trends in Technology and Intellectual Property in Brazil* (2014). He is an officer of the Brazilian Association of Information Technology and Telecommunications Law (ABDTIC).

**MARcin Lewoszewski**  
*Kobyłaska & Lewoszewski Kancelaria Prawna Sp J*

Marcin Lewoszewski is a legal counsel, member of the Warsaw Bar Associations. Before establishing his own law firm, he worked for more than seven years in the TMT team with one of the leading international law firms based in Warsaw. Before that, for two years, he worked at the Inspector’s General Office for Personal Data Protection (GIODO). He is co-chair of the IAPP KnowledgeNET for Poland.

Marcin specialises in legal advice on personal data protection and the law of new technologies, including the provision of electronic services, database protection, gambling, IT systems implementation and telecommunications law. He advised clients in locating data processing centres in Poland and participated in creating one of the largest online B2B trading platforms in Poland. He has many years of experience in leading projects aimed at adapting business practices to the requirements of the data protection law. On numerous occasions, he represented clients in proceedings conducted by the Inspector General for Personal Data Protection, including for the acceptance of binding corporate rules by the supervisory authority, and in connection with GIOD0 (the DPA) inspections. His experience includes negotiating database licence agreements, as well as advising clients on the legal aspects of obtaining data from publicly available records. His professional interests focus on selected sectors of the economy, primarily pharmaceuticals, e-commerce, new technologies, and media.

**William RM Long**  
*Sidley Austin LLP*

William Long is a global co-leader of Sidley’s highly ranked privacy and cybersecurity practice and also leads the EU data protection practice at Sidley. William advises international clients on a wide variety of GDPR, data protection, privacy, information security, social media, e-commerce and other regulatory matters.

William has been a member of the European Advisory Board of the International Association of Privacy Professionals (IAPP) and on the DataGuidance panel of data
William was previously in-house counsel to one of the world’s largest international financial services groups. He has been a member of a number of working groups in London and Europe looking at the EU regulation of e-commerce and data protection. He holds a JD from Columbia Law School and a BA from the University of California, Berkeley.

LETRICIA LÓPEZ-LAPUENTE

_Luría Menéndez Abogados, SLP_

Leticia López-Lapuente is a lawyer in the Madrid office of Spanish law firm Luría Menéndez. She heads the firm’s data protection and IT practice, and leads the LATAM data protection group.

Leticia focuses her practice on data protection, commercial and corporate law, especially in the internet, software, e-commerce and technology sectors. She also advises on privacy law issues. Leticia provides clients operating in these sectors with day-to-day advice on regulatory, corporate and commercial matters, including the drafting and negotiation of contracts, M&A, privacy advice, consumer protection and e-commerce issues, corporate housekeeping, public procurement and RFP procedures, and dealings with public authorities. She has been involved in major transactions and assisted businesses and investors in these sectors.

She regularly speaks in national and international fora regarding personal data protection and technology, in addition to having written numerous articles on data protection-related matters.

ANETA MIŚKOWIEC

_Kobyłańska & Lewoszewski Kancelaria Prawna Sp J_

Aneta Miśkowiec is a lawyer, University of Warsaw law graduate. Before joining Kobyłańska & Lewoszewski, Aneta worked in an international law firm, dealing with issues of various areas of law. Aneta supports the team in the practice of personal data protection and intellectual property law as part of the implementation of the obligations resulting from the General Data Protection Regulation. Aneta defended her master’s thesis on personal data protection under the title ‘Privacy Impact Assessment’ and took second place in the seventh edition of the essay competition for students, organised by the Polish data protection authority.

VIVEK K MOGAN

_Sidley Austin LLP_

Vivek K Mohan is senior privacy and cybersecurity counsel at Apple Inc, where he is responsible for privacy and security issues associated with Apple’s products, services and corporate infrastructure. He joined Apple from the privacy, data security and information law group at Sidley Austin LLP, where he counselled clients in the technology, telecommunications, healthcare and financial services sectors. Mr Mohan is the co-editor and author of the PLI treatise ‘Cybersecurity: A Practical Guide to the Law of Cyber Risk’, published in September 2015. He has worked as an attorney at Microsoft, at the Internet Bureau of the New York State Attorney General (under a special appointment) and at General Electric’s
corporate headquarters (on secondment). For five years, Mr Mohan was a resident fellow and later a non-resident associate with the Cybersecurity Project at the Harvard Kennedy School.

MICHAEL MORRIS

Allens

Michael is an expert telecommunications, technology, intellectual property and data protection lawyer, and is well known for staying on the cutting edge of legal developments in these areas for corporate and government clients in Australia. He is particularly experienced in large projects and transactions involving the procurement and delivery of ICT, business process outsourcing and ICT systems separations and business transformations. He is part of Allens’ leading practice advising on management of the full data life cycle, particularly the use, exchange, monetisation and protection of data, and he regularly advises clients across all industry sectors and the government on data security, privacy and associated issues.

ALAN CHARLES RAUL

Sidley Austin LLP

Alan Raul is the founder and lead global coordinator of Sidley Austin LLP’s highly ranked privacy and cybersecurity practice. He represents companies on federal, state and international privacy issues, including global data protection and compliance programmes, data breaches, cybersecurity, consumer protection issues and internet law. Mr Raul’s practice involves litigation and acting as counsel in consumer class actions and data breaches, as well as FTC, state attorney general, Department of Justice and other government investigations, enforcement actions and regulation. Mr Raul provides clients with perspective gained from extensive government service. He previously served as vice chair of the White House Privacy and Civil Liberties Oversight Board, general counsel of the Office of Management and Budget, general counsel of the US Department of Agriculture and associate counsel to the President. He currently serves as a member of the Data Security, Privacy & Intellectual Property Litigation Advisory Committee of the US Chamber Litigation Center (affiliated with the US Chamber of Commerce). Mr Raul also serves as a member of the American Bar Association’s Cybersecurity Legal Task Force by appointment of the ABA president. He is also a member of the Council on Foreign Relations. Mr Raul holds degrees from Harvard College, Harvard University’s Kennedy School of Government and Yale Law School.

HUGH REEVES

Walder Wyss Ltd

Hugh Reeves is an associate in the information technology, intellectual property and competition team of the Swiss law firm Walder Wyss Ltd. His preferred areas of practice include technology transfers, data protection and privacy law, as well as information technology and telecommunications law. He is also active in the areas of copyright, patent, trademark and trade secret law.

Hugh Reeves was educated at the University of Lausanne (BLaw, 2008; MLaw, 2010) and the University of California at Berkeley (LLM, 2016).
GÉRALDINE SCALI  
_Sidley Austin LLP_
Géraldine Scali is a counsel in the London office of Sidley Austin LLP, whose main practice areas are data protection, privacy, cybersecurity, e-commerce and information technology.

JÜRG SCHNEIDER  
_Walder Wyss Ltd_
Jürg Schneider is a partner with the Swiss law firm Walder Wyss Ltd. Jürg Schneider’s practice areas include information technology, data protection and outsourcing. He regularly advises both Swiss and international firms on comprehensive licensing, development, system integration and global outsourcing projects. He has deep and extensive experience in the fields of data protection, information security and e-commerce, with a particular focus on transborder and international contexts. Jürg Schneider is a member of the board of directors of the International Technology Law Association and immediate past co-chair of its data protection committee. In addition, Jürg Schneider regularly publishes and lectures on ICT topics in Switzerland and abroad.

Jürg Schneider was educated at the University of Neuchâtel (lic iur 1992, Dr iur 1999). He has previously worked as a research assistant at the University of Neuchâtel, as a trainee at the legal department of the canton of Neuchâtel and in a Neuchâtel law firm.

Jürg Schneider speaks German, French and English. He is registered with the Zurich Bar Registry and admitted to practise in all of Switzerland.

STEVEN DE SCHRIJVER  
_Astrea_
Steven De Schrijver is a partner in the Brussels office of Astrea. He has more than 25 years of experience advising some of the largest Belgian and foreign technology companies, as well as innovative entrepreneurs on complex commercial agreements and projects dealing with new technologies. His expertise includes e-commerce, software licensing, website development and hosting, privacy law, IT security, technology transfers, digital signatures, IT outsourcing, cloud computing, advertising, drones, robotics and social networking.

Steven has also been involved in several national and cross-border transactions in the IT, media and telecom sectors. He participated in the establishment of the first mobile telephone network in Belgium, the establishment of one of the first e-commerce platforms in Belgium, the acquisition of the Flemish broadband cable operator and network, and the acquisition and sale of several Belgian software and technology companies. He has also been involved in numerous outsourcing projects and data protection (now GDPR) compliance projects.

Steven is the Belgian member of EuroITCounsel, a quality circle of independent IT lawyers. He is also a board member of ITechLaw and the International Federation of Computer Law Associations. In 2012, 2014, 2017 and 2018 he was awarded the Global Information Technology Lawyer of the Year award by _Who’s Who Legal_ and, in 2012, he received the ILO Client Choice Award in the corporate law category for Belgium.

Steven has been admitted to the Brussels Bar. He holds a law degree from the University of Antwerp (1992) and an LLM degree from the University of Virginia School of Law (1993). He obtained his CIPP/E certification in 2018.
OLGA STEPANOVA
Winheller Rechtsanwaltsgesellschaft mbH

Olga Stepanova heads the IP/IT department at Winheller Attorneys at Law & Tax Advisors, where she advises German and international companies and non-profit organisations on issues of data protection, IT law and intellectual property. She also provides legal counsel in German and international copyright, trademark and media law matters. As member of Winheller’s Russian desk, she advises her Russian clients in their mother tongue.

MONIQUE STURNY
Walder Wyss Ltd

Monique Sturny is a managing associate in the information technology, intellectual property and competition team of the Swiss law firm Walder Wyss Ltd. She advises international and domestic companies on data protection law, competition law, distribution law, contract law and information technology law matters, as well as with respect to the setting up of compliance programmes. She represents clients in both antitrust and data protection proceedings in court and before administrative bodies. She regularly publishes and speaks at conferences in her areas of practice.

Monique Sturny was educated at the University of Fribourg (lic iur, 2002), the London School of Economics and Political Science (LLM in international business law, 2007) and the University of Berne (Dr iur, 2013).

ADITI SUBRAMANIAM
Subramaniam & Associates

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 (LLM), from Columbia University, New York, United States. She specialises in patent and trade mark 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 cybersecurity. She is widely published and very well regarded in the Indian and international legal fraternity.

YUET MING THAM
Sidley Austin LLP

Yuet is a global head of the government litigation and investigations group, and head of the Asia-Pacific compliance and investigations group. Besides compliance and investigations, Yuet focuses on privacy and cybersecurity work. She speaks fluent English, Mandarin, Cantonese and Malay and is admitted in New York, England and Wales, Hong Kong, and Singapore.

Yuet was most recently awarded the Emerging Markets ‘compliance and investigations lawyer of the year’ by The Asian/American Lawyer, with the team also recognised as the ‘compliance/investigations firm of the year’. She has also been acknowledged as a ‘leading lawyer’ by Chambers Asia-Pacific across four categories namely ‘dispute resolution: litigation,’ ‘corporate investigations/anti-corruption,’ ‘life sciences’ and ‘financial services: contentious regulatory.’ Additionally, Yuet is recognised in the ‘financial services regulatory’ in IFLR1000 as

© 2018 Law Business Research Ltd
a ‘leading lawyer’ and has also been listed by Who’s Who Legal as a ‘leading business lawyer’ in ‘life sciences,’ ‘business crime defense’ and ‘investigations.’ In the 2018 edition of *Chambers Asia-Pacific*, Yuet is described as ‘exceptionally bright’ and ‘very responsive and knowledgeable and can immediately dive into the issues’. The 2015 edition of *Chambers Global* stated ‘Ms Tham is described by clients as “a marvellous and gifted attorney”’. Meanwhile, *Chambers Asia-Pacific* noted that Yuet ‘is frequently sought after by international corporations, who respect her experience and expertise in risk management’.

**ALAN CAMPOS ELIAS THOMAZ**  
*Mattos Filho, Veiga Filho, Marrey Jr e Quiroga Advogados*

Alan Thomaz is an associate of Mattos Filho’s intellectual property and technology practice, where he focuses on IP and technology matters related to privacy, data protection and cybersecurity, information technology, cloud services and e-commerce, among others. He is co-author of several books on privacy and data protection, and is a member of the International Association of Privacy Professionals (IAPP), with certification on European data protection law (CIPP/E), the International Chamber of Commerce (ICC), the Interactive Advertising Bureau (IAB) and the Brazilian Intellectual Property Association (ABPI).

**FRANCISCO ZAPPA**  
*M&M Bomchil*

Francisco Zappa is a semi-senior lawyer in the mergers and acquisitions and entertainment law departments. He joined M&M Bomchil in 2011.

He graduated with honours from the University of Salvador, Buenos Aires and completed his masters’ degree in corporate law at the University of San Andrés, Buenos Aires. His practice focuses on diverse corporate and contractual matters. He has wide experience in fair trade and consumer protection issues and specialises in data protection law.

During 2017, he was an international associate at the New York offices of Simpson Thacher & Bartlett.

He is a frequent speaker at chambers of commerce on matters in his areas of expertise.

**SELEN ZENGIN**  
*BTS&Partners*

Selen Zengin graduated from Istanbul Bilgi University, faculty of law in 2016 and was admitted to the Istanbul Bar Association in 2018. She particularly specialises in data protection and electronic communications as well as cybersecurity, digital advertising and legal technology sectors. Selen provides consultancy to local and international clients during the processes of negotiating, reviewing and drafting of legal instruments and prepares regulatory and technical compliance reports.
Appendix 2

CONTRIBUTING LAW FIRMS’ CONTACT DETAILS

**ALLENS**
Level 26
480 Queen Street
Brisbane Queensland 4000
Australia
Tel: +61 7 3334 3000
Fax: +61 7 3334 3444
michael.morris@allens.com.au
www.allens.com.au

**ASTREA**
Louizalaan 235
1050 Brussels
Belgium

Posthofbrug 6
2600 Berchem
Antwerp
Belgium

Tel: +32 2 215 97 58
Fax: +32 2 216 50 91
sds@astrealaw.be
www.astrealaw.be

**BTS&PARTNERS**
Esentepe Mah
23 Temmuz Sok. No:2 34394
Şişli
Istanbul
Turkey
Tel: +90 212 292 7934 / +90 212 245 0801
Fax: +90 212 292 7939 / +90 212 251 6719
info@bts-legal.com
batu.kinikoglu@bts-legal.com
selen.zengin@bts-legal.com,
kaancan.akdere@bts-legal.com
www.bts-legal.com

**JUN HE LLP**
20/F, China Resources Building
8 Jianguomenbei Avenue
Beijing 100005
China
Tel: +86 10 8519 1718
Fax: +86 10 8519 1350
dongx@junhe.com
www.junhe.com

**BOGSCH & PARTNERS LAW FIRM**
Maros utca 12
1122 Budapest
Hungary
Tel: +36 1 318 1945
Fax: +36 1 318 7828
tamas.godolle@bogsch.hu
www.bogsch.hu
Contributing Law Firms’ Contact Details

KOBYŁAŃSKA & LEWOSZEWSKI KANCELARIA PRAWNA SP J
ul. Wspólna 50/11
00-684 Warsaw
Poland
Tel: +48 22 25 34567
kancelaria@klattorneys.pl
marcin.lewoszewski@klattorneys.pl
anna.kobylanska@klattorneys.pl
aneta.miskowiec@klattorneys.pl
maja.karczewska@klattorneys.pl
www.klattorneys.pl

M&M BOMCHIL
Suipacha 268, 12th floor
Buenos Aires 1008
Argentina
Tel: +54 11 4321 7500
Fax: +54 11 4321 7555
adrian.furman@bomchil.com
mercedes.deartaza@bomchil.com
francisco.zappa@bomchil.com
www.bomchil.com.ar

MÁRQUEZ, BARRERA, CASTAÑEDA & RAMÍREZ
Cra 11A No. 97A-19 Of 401
Bogotá
Colombia
Tel: +57 1 675 3548
nbbarrera@marquezbarrera.com
www.marquezbarrera.com

MATHESON
70 Sir John Rogerson’s Quay
Dublin 2
Ireland
Tel: +353 1 232 2000
Fax: +353 1 232 3333
anne-marie.bohan@matheson.com
www.matheson.com

MATTOS FILHO, VEIGA FILHO, MARREY JR E QUIROGA ADVOGADOS
Alameda Joaquim Eugênio de Lima 447
São Paulo 01403-001
Brazil
Tel: +55 11 3147 7600
kujawski@mattosfilho.com.br
alan.thomaz@mattosfilho.com.br
www.mattosfilho.com.br

NNOVATION LLP
251 Laurier Avenue West, Suite 900
Ottawa
Ontario K1P 5J6
Canada
Tel: +1 613 656 1297
Fax: +1 888 314 5997
sbrown@nnovation.com
www.nnovation.com

NOERR
1-ya Brestskaya ul. 29
Moscow 125047
Russia
Tel: +7 495 7995696
Fax: +7 495 7995697
vyacheslav.khayryuzov@noerr.com
www.noerr.com

SANTAMARINA Y STETA, SC
Av Ricardo Margáin Zozaya 335
Tower I, floor 7
Valle del Campestre
66265 Garza García
Nuevo León
Mexico
Tel: +52 81 8133 6000 / 6002
Fax: +52 81 8368 0111
crcruz@s-s.mx
dacosta@s-s.mx
www.s-s.mx

© 2018 Law Business Research Ltd
SIDLEY AUSTIN LLP
39/F Two International Finance Centre
Central
Hong Kong
Tel: +852 2509 7645
Fax: +852 2509 3110
Level 31, Six Battery Road
Singapore 049909
Tel: +65 6230 3969
Fax: +65 6230 3939
yuetming.tham@sidley.com

Woolgate Exchange
25 Basinghall Street
EC2V 5HA
London
United Kingdom
Tel: +44 20 7360 3600
Fax: +44 20 7626 7937
wlong@sidley.com
gscali@sidley.com
fblythe@sidley.com

199 Avenue of the Stars, 17th floor
Los Angeles
California 90067
United States
Tel: +1 310 595 9500
Fax: +1 310 595 9501
ecooper@sidley.com
sheri.rockwell@sidley.com

1501 K Street, NW
Washington, DC 20005
United States
Tel: +1 202 736 8000
Fax: +1 202 736 8711
araul@sidley.com

Sidley Austin Nishikawa Foreign Law Joint Enterprise
Marunouchi Building 23F 4-1
Marunouchi 2-Chome
Chiyoda-ku
Tokyo 100-6323
Japan
Tel: +81 3 3218 5900
Fax: +81 3 3218 5922
tishiara@sidley.com

www.sidley.com

SK CHAMBERS
9B Jalan Setiapusa
Bukit Damansara
50490 Kuala Lumpur
Malaysia
Tel: +60 3 2011 6800
Fax: +60 3 2011 6801
sk@skchambers.co
www.skchambers.co

SUBRAMANIAM & ASSOCIATES
M3M Cosmopolitan, 7th Floor
Sector 66, Golf Course Extension Road
Gurugram – 122001
National Capital Region
India
Tel: +91 124 4849700
Fax: +91 124 4849798 / 4849799
sna@sna-ip.com

URÍA MENÉNDEZ ABOGADOS, SLP
c/Príncipe de Vergara, 187
Plaza de Rodrigo Uria
28002 Madrid
Spain
Tel: +34 915 860 131
Fax: +34 915 860 403
leticia.lopez-lapuente@uria.com
reyes.bermejo@uria.com
www.uria.com
WALDER WYSS LTD
Seefeldstrasse 123
PO Box 1236
8034 Zurich
Switzerland
Tel: +41 58 658 58 58
Fax: +41 58 658 59 59
juerg.schneider@walderwyss.com
monique.sturny@walderwyss.com
hugh.reeves@walderwyss.com
www.walderwyss.com
www.dataprotection.ch

WINHELLER
RECHTSANWALTSGESELLSCHAFT
MBH
Tower 185
Friedrich-Ebert-Anlage 35–37
60327 Frankfurt
Germany
Tel: +49 69 76 75 77 80
Fax: +49 69 76 75 77 810
info@winheller.com
www.winheller.com