THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

SIXTH EDITION

Editor
Alan Charles Raul

THE LAWREVIEWS

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

Sixth Edition

Reproduced with permission from Law Business Research Ltd
This article was first published in October 2019
For further information please contact Nick.Barette@thelawreviews.co.uk

Editor
Alan Charles Raul

THE LAWREVIEWS

PUBLISHER
Tom Barnes

SENIOR BUSINESS DEVELOPMENT MANAGER
Nick Barette

BUSINESS DEVELOPMENT MANAGER
Joel Woods

SENIOR ACCOUNT MANAGERS
Pere Aspinall, Jack Bagnall

ACCOUNT MANAGERS
Olivia Budd, Katie Hodgetts, Reece Whelan

PRODUCT MARKETING EXECUTIVE
Rebecca Mogridge

RESEARCH LEAD
Kieran Hansen

EDITORIAL COORDINATOR
Tommy Lawson

HEAD OF PRODUCTION
Adam Myers

PRODUCTION EDITOR
Anna Andreoli

SUBEDITOR
Charlotte Stretch

CHIEF EXECUTIVE OFFICER
Nick Brailey

Published in the United Kingdom
by Law Business Research Ltd, London
Meridian House, 34-35 Farringdon Street, London, EC2A 4HL, UK

www.TheLawReviews.co.uk

ISBN 978-1-83862-062-2

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

© 2019 Law Business Research Ltd

ACKNOWLEDGEMENTS

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

ALLENS

ANJIE LAW FIRM

ASTREA

BOGSCH & PARTNERS LAW FIRM

BOMCHIL

BTS&PARTNERS

CLEMENS

KOBYLAŃSKA LEWOSZEWSKI MEDNIS SP. J.

MÁRQUEZ, BARRERA, CASTAÑEDA & RAMÍREZ

NNOVATION LLP

NOERR

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SK CHAMBERS

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

VUKINA & PARTNERS LTD

WALDER WYSS LTD

WINHELLER ATTORNEYS AT LAW & TAX ADVISORS

CONTENTS

Chapter 1

GLOBAL OVERVIEW

Alan Charles Raul[1]

IS DIGITAL GOVERNANCE THE NEW STANDARD?

Following the first year of life under the EU's General Data Protection Regulation (GDPR), and with only months to go until the California Consumer Privacy Act (CCPA) goes into effect, 2019 feels more like *Waiting for Godot* than *Hallelujah Chorus*. Everyone says they want US federal privacy legislation but there is considerable contention as to whether it should emulate the GDPR, pre-empt the CCPA or stake out a new track to protect people's privacy and digital rights against genuine abuses. Unless policy makers around the world make a real effort to identify the actual privacy risks people face, we will see more of the same in 2020 – an incessant barrage of tedious cookie notices, overwrought haranguing against tailored advertising and more blaming of victims of cybercrime for governments' failure to protect their economies from electronic attack by sophisticated state actors and criminals.

Accordingly, uncertainty abounds in the digital realm. In addition to policy stasis in Washington, the long-awaited Indian data protection law continues to elude finalisation. The application and interpretation of China's Cybersecurity Law, draft privacy requirements and potential enforcement appear designed to confound international business. And the future of the EU's next shoe to drop – an ePrivacy Regulation for the communications sector – remains equivocal.

Having said that, some highly consequential digital developments have occurred in the last year (in addition to the CCPA earthquake out of California). Canada's mandatory data breach notification requirements went into effect in November 2018. Spain's Data Protection Law introduced a slate of new 'digital rights' relating to new technologies – rights that are distinct from privacy or data protection rights. In particular, the new law imposes a duty on providers of information society services and social networks to rectify misinformation on the internet. This new duty for tech companies would appear to be similar to what the UK proposed in its April 2019 'Online Harms' White Paper (which was open for public comments until July 2019). Interestingly, the new Spanish law also introduced a 'digital disconnection right' designed to guarantee that workers and civil servants will be able to stop looking at their work devices during break time, leave and holidays.

While the UK and France have imposed or proposed massive fines of £99 million for a data breach and €50 million for 'lack of transparency, inadequate [disclosure of] information and lack of valid consent regarding the ads personalization', the biggest enforcement developments did not emanate from the EU under the GDPR's new authority to issue penalties of 4 per cent of annual global revenue. Instead, US federal and state regulators

1 Alan Charles Raul is a partner at Sidley Austin LLP.

imposed hundreds of millions of dollars in fines on companies that suffered data breaches. But it was the FTC that imposed the largest fine by any privacy regulator ever on Facebook in the aftermath of *Cambridge Analytica*. The Federal Trade Commission's (FTC) fine of US$5 billion was 200 times larger than the FTC's previous high for a privacy penalty, 20 times larger than any prior privacy penalty anywhere in the world and amounted to approximately 9 per cent of the company's global annual revenue in the previous year.

Nonetheless, privacy advocates claimed this unprecedented penalty was still too low. Perhaps such analysts were simply channelling FTC Commissionner Rohit Chopra, who explained, candidly, that he dissented from the agency's settlement because it would do 'little to change the [behavioral advertising] business model.'

In contrast, FTC Chairman Joe Simons and Commissioners Noah Joshua Phillips and Christine S Wilson issued a statement supporting the settlement in which they said that 'the magnitude of this penalty resets the baseline for privacy cases . . . and sends a strong message to every company in America that collects consumers' data: where the FTC has the authority to seek penalties, it will use that authority aggressively'.

Perhaps most significant, though, was the FTC's imposition of a highly regimented and rigorous new privacy governance structure. The FTC described these new governance requirements as 'overhaul[ing] the way the company makes privacy decisions by boosting the transparency of decision making and holding Facebook accountable via overlapping channels of compliance.'

The company itself appeared to accept the agency's perspective that the new mandate for privacy governance 'will require a fundamental shift in the way we approach our work and it will place additional responsibility on people building our products at every level of the company.' The company also noted that the 'accountability required by this agreement surpasses current US law' and expressed the hope that the settlement agreement will 'be a model for the industry,' noting that 'it introduces more stringent processes to identify privacy risks, more documentation of those risks, and more sweeping measures to ensure that we meet these new requirements'.

In announcing the settlement, the FTC highlighted the following governance elements in its announcement of the settlement.

a '[G]reater accountability at the board of directors level', including the establishment of an independent privacy committee of Facebook's board of directors, with an independent nominating committee responsible for appointing the members of the privacy committee and a supermajority of the Facebook board of directors required to fire any of them.

b Improved 'accountability at the individual level', including by requiring Facebook to 'designate compliance officers who will be responsible for Facebook's privacy program' and by requiring the CEO and designated compliance officers independently 'to submit to the FTC quarterly certifications that the company is in compliance with the privacy program mandated by the order, as well as an annual certification that the company is in overall compliance with the order', with false certification subjecting them to individual civil and criminal penalties.

c 'Strengthen[ed] external oversight of Facebook', by enhancing the 'independent third-party assessor's ability to evaluate the effectiveness of Facebook's privacy program and identify any gaps'.

d A mandatory 'privacy review of every new or modified product, service, or practice before it is implemented, and document[ation of] its decisions about user privacy'. This means that:

- compliance officers must generate a 'quarterly privacy review report, which they must share with the CEO and the independent assessor, as well as with the FTC upon request by the agency';
- Facebook must 'exercise greater oversight over third-party apps, including by terminating app developers that fail to certify that they are in compliance with Facebook's platform policies or fail to justify their need for specific user data';
- Facebook must 'implement procedures designed to ensure that Covered Information entered by the User (such as User-generated content) is deleted from servers under [Facebook]'s control, or is de-identified such that it is no longer associated with the User's account or device, within a reasonable period of time (not to exceed 120 days) from the time that the User has deleted such information, or his or her account' subject to certain exceptions;
- Facebook must give 'clear and conspicuous notice of its use of facial recognition technology, and obtain affirmative express user consent prior to any use that materially exceeds its prior disclosures to users'; and
- Facebook must 'establish, implement, and maintain a comprehensive data security program'.

In all, 2019 has produced more privacy policy questions than answers, but through their large fines and mandated new business practices the world's data protection regulators certainly managed to command the attention of corporate leaders and investors.

Finally, the global data protection community lost a great man and leading privacy philosopher when Giovanni Buttarelli passed away in August. Giovanni, an Italian jurist and scholar, served as European Data Protection Supervisor at the time of his death. In October 2018, Giovanni chaired the brilliantly successful 40th anniversary International Conference of Data Protection and Privacy Commissioners in Brussels. The themes of the conference were 'Debating Ethics: Dignity and Respect in a Data Driven Life' and 'Choose Humanity: Putting Dignity Back into Digital.' In his opening speech, Giovanni explained:

> *. . . that we are now living through a new generational shift in the respect for privacy. This shift is towards establishing a sustainable ethics for a digitised society. It is driven by the globalisation of the economy, and the socio-technological forces . . . It is driven by the digitisation of almost everything in our economy and services sector, our social relations, politics and government. Above all, it is driven by the prospect of human decision-making, responsibility and accountability being delegated to machines. Digitisation respects no geographical boundaries. Digitisation is not sensitive to human boundaries between what we want to be public, private or something in between. It injects itself into our most intimate spaces – relationships, communications and attention. The so-called 'privacy paradox' is not that people have conflicting desires to hide and to expose. The paradox is that we have not yet learned how to navigate the new possibilities and vulnerabilities opened up by rapid digitisation. What do I mean by ethics? Ethics is the sense we all have, often subconscious, of right and wrong in different circumstances. Philosophers on this stage will shortly explain how ethical consensuses have emerged in the past. In today's digital sphere, however, there is no such ethical consensus. We do not have a consensus in Europe, and we certainly do not have one at a global level. But we urgently need one.*

Whereas today's privacy rules and regulations – especially from Europe – may in fact be more burdensome than is necessary or desirable, they may still not get to the heart of the matter: as Giovanni opined, we must seek an ethical consensus of right and wrong for the digital sphere. It is no small undertaking to achieve this at a global level. And now it will be that much harder without Giovanni Buttarelli to help lead the way.

Chapter 2

EU OVERVIEW

William RM Long, Géraldine Scali, Francesca Blythe and Alan Charles Raul[1]

I OVERVIEW

In the EU, data protection is principally governed by the EU General Data Protection Regulation (GDPR),[2] which came into force on 25 May 2018 and is applicable in all EU Member States. The GDPR repealed the Data Protection Directive 95/46/EC (Directive),[3] regulates the collection and processing of personal data across all sectors of the EU economy and introduced new data protection obligations for controllers and processors alongside new rights for EU individuals.

The GDPR 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.

In March 2019, the European Data Protection Board's (EDPB) published its first overview on the implementation of the GDPR. The overview provided statistics on the consistency mechanism, the cooperation mechanism and enforcement under the GDPR. In particular, as at the time of publication the total number of cases reported by DSAs from 31 EEA countries totalled 206,326 with 94,622 of these constituting complaints and 64,684 initiated as a data breach notification. In addition, DSAs from 11 EEA countries reported imposing administrative fines under the GDPR totalling €55,955,871. In May 2019, the European Data Protection Board's (EDPB) published further statistics noting that DSAs had logged over 144,000 queries and complaints, and over 89,000 data breaches.

Set out in this chapter is a summary of the main provisions of the GDPR. We then cover guidance provided by the EU's former Article 29 Working Party (which has, since 25 May 2018, been replaced by the 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).

---

1 William RM Long and Alan Charles Raul are partners, Géraldine Scali is a counsel and Francesca Blythe is a senior associate at Sidley Austin LLP.

2 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

3 European Parliament and Council Directive 95/46/EC 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.

II THE GDPR

The GDPR imposes a number of obligations on organisations processing the personal data of individuals (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.

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 EU, or, where the controller or processor does not have an establishment in the EU, but processes personal data in relation to the offering of goods or services to individuals in the EU; or the monitoring of the behaviour of individuals in the EU as far as their behaviour takes place within the EU.

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

The EDPB published its draft guidance on the territorial application of the GDPR in November 2018 that was subject to public consultation until January 2019. The draft guidance largely reaffirms prior interpretations but it does leave some legal uncertainty for non-EU organisations including on how to deal with the GDPR's international data transfer restrictions. It is hoped that these concerns will be addressed once the finalised guidance is published.

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. Interestingly, a recent decision from the CJEU (decided under the former Directive) considered the question of joint controllership. In particular, the CJEU held that for there to be a relationship of joint control, the parties do not need to share responsibility equally, nor do they have to have access to the personal data processed. Unfortunately the ruling does not address the question of liability between the parties;

b 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;

4 Article 3(2) of the GDPR.

5 Article 4 of the GDPR.

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 considered personal data under the GDPR; and

g 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 of controllers and processors under the GDPR

Notification

The notification obligation under the Directive requiring controllers to notify their national DSA 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 DSA, 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 (and processors) to maintain a record of their processing activities. For controllers, this record 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 retention 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.

6 Recital 22 of the GDPR.

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:[7] personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject;

b the purpose limitation principle:[8] 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:[9] 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:[10] 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;

e storage limitation principle:[11] 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;

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

g 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, when using new technologies and 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

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.

11 Article 5(1)(e) of the GDPR.

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.

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;

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 EDPB 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 EDPB 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 risk[13] 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

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.

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);

e data processed on a large scale: the GDPR does not define what constitutes large-scale. In any event, the EDPB 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.

f 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;

g 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

h 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.

i 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 EDPB 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 EDPB recommends that as a matter of good practice, controllers should continuously review and regularly reassess their DPIAs.[15]

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 a DPO 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 EDPB, in its guidance on DPOs, noted 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

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.

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

'inextricable' part of the controller or processor's activities. The EDPB 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 EDPB 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]

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.[21] 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.[22]

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.[23]

The EDPB 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.[24]

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 29 Working Party Guidelines on Data Protection Officers ('DPOs'), WP 243. as last revised and adopted on 5 April 2017, page 12.

20 Article 37(7) of the GDPR.

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.

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. The EDPB published draft guidelines on this lawful ground in April 2019 in which a very narrow interpretation of contractual necessity was adopted;

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.[25]

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 (special categories of personal data) can only be processed where both a lawful ground under Article 6 and a condition under Article 9 are satisfied. The Article 9 conditions that are most often 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 EDPB states in its guidance on consent, that where controllers intend to rely on consent as a lawful ground for processing, they have a duty to assess whether they will meet all of the GDPR requirements to obtain valid consent.[26] 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 EDPB notes, consent can only be an appropriate lawful ground 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.[27] Without such genuine and free choice, the EDPB notes the data subject's consent becomes illusory and consent will be invalid, rendering the processing unlawful.[28]

25 Article 6 of the GDPR.

26 Article 29 Working Party, Guidelines on consent under Regulation 2016/679, WP259, as last revised and adopted on 10 April 2018, page 3.

27 ibid.

28 ibid.

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:

a the identity and contact details of the controller (and where applicable, the controller's representative);
b the contact details of the DPO, where applicable;
c the purposes of the processing;
d the lawful ground for the processing;
e the recipients or categories of recipients of the personal data;
f 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;
g the period for which the personal data will be stored or where that is not possible, the criteria used to determine that period;
h the existence of rights of data subjects to access, correct, restrict and object to the processing of their personal data;
i the right to lodge a complaint with a DSA; and
j 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 and types of 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.[29] 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 EU or Member State law or obtaining or disclosing of personal data is expressly laid down by EU or Member State law to which the controller is subject.[30] These exceptions, according to the EDPB should be interpreted narrowly.[31]

The EDPB 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]

29 Article 14(3) of the GDPR.

30 Article 14(5) of the GDPR.

31 Article 29 Working Party Guidelines on transparency under Regulation 2016/679, as last revised and adopted on 11 April 2018, page 25.

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

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 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 processor under which the 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 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 EDPB on personal data breach notification under the GDPR[35] 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.

33 Article 32 of the GDPR

34 Article 28(4) of the GDPR.

35 Article 29 Data Protection Working Party Guidelines on Personal Data Breach Notification under Regulation 2016/679, WP 250, as last revised and adopted on 6 February 2018, page 7.

The EDPB notes 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 EDPB provides 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 EDPB notes 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 EDPB, 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:

a Type of personal data breach: is it a confidentiality, availability, or integrity type of breach?

b 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.

c 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.

d 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.

e 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.

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

g 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.

h Other general considerations: assessing the risk associated with a breach can be far from straightforward. Therefore the EDPB, 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.[39]

36 Article 29 Data Protection Working Party Guidelines on Personal Data Breach Notification under Regulation 2016/679, WP 250, as last revised and adopted on 6 February 2018, page 12.

37 ibid.

38 ibid.

39 Article 29 Data Protection Working Party Guidelines on Personal Data Breach Notification under Regulation 2016/679, WP 250, as last revised and adopted on 6 February 2018, page 26.

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 and/or processors may not transfer personal data to countries outside of the European Economic Area (EEA)[40] unless the recipient country provides an adequate level of protection for the personal data.[41] 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, Japan, Jersey, New Zealand, Switzerland and Uruguay. In addition, 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 organisations in the EU.[42] On 11 June 2018, 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 by 1 September 2018, 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 contained in the Privacy Shield. The second annual review of the functioning of the Privacy Shield was published by the European Commission on 19 December 2018, also asking the US to appoint a permanent Privacy Shield ombudsman by 28 February 2019. On 18 January 2019, the US announced its intention to appoint Keith Krach as the Privacy Shield's first permanent ombudsman. Mr Krach's nomination was confirmed by the US Senate on 20 June 2019. The validity of the Privacy Shield has also been challenged before the CJEU by the French digital privacy rights advocacy group, La Quadrature du Net, claiming the Privacy Shield is incompatible with

40 The EEA consists of the 28 EU Member States together with Iceland, Liechtenstein and Norway.

41 Article 45 of the GDPR.

42 Commission Implementing Decision (EU) 2016/1250 of 12 July 2016.

EU data protection laws, given the potential access to the transferred personal data by US surveillance agencies. The CJEU has, however, postponed the hearing of this case pending judgment in the case before the CJEU concerning the validity of model contracts (see below).

Where transfers are to be made to countries that are not deemed adequate, other exceptions may apply to permit the transfer.[43] The European Commission has approved EU 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).[44] 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 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 DSA, the Irish High Court referred the questions to the CJEU for a preliminary ruling to determine the legal status of model contracts. The CJEU is expected to give its judgment in early 2020. Separately, the European Commission recently announced that it is working to modernise model contracts, but this is unlikely to be completed before the CJEU publishes its judgment.

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 EDPB has published various documents[45] on binding corporate rules, including a model checklist for the approval of binding corporate rules,[46] a table setting out the elements and principles to be found in binding corporate

43 Article 46 of the GDPR.

44 Article 46(2)(c) of the GDPR.

45 WP 133 – Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data adopted on 10 January 2007.
WP 154 – Working Document setting up a framework for the structure of Binding Corporate Rules adopted on 24 June 2008.
WP 155 – Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules adopted on 24 June 2008 and last revised on 8 April 2009.
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 204 – Explanatory Document on the Processor Binding Corporate Rules last revised and adopted on 22 May 2015.

46 WP 108 – Working Document establishing a model checklist application for approval of binding corporate rules adopted on 14 April 2005.

rules,[47] an explanatory document on processor binding corporate rules, recommendations on the standard application for approval of controller and processor binding corporate rules,[48] a co-operation procedure for issuing common opinions on adequate safeguards resulting from binding corporate rules, a framework for the structure of binding corporate rules, and frequently asked questions on 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.

Timing and costs

The GDPR requires that a data subject's request to exercise their rights 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.

47 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.

48 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.
WP 265 – Recommendation on the Standard Application form for Approval of Processor Binding Corporate Rules for the Transfer of Personal Data – Adopted on 11 April 2018.

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.[49] 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 information or processing activities to which the request relates.[50] 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.[51] 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.[52]

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.[53]

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:

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;[54]

49 Article 15(4) of the GDPR.

50 Recital 63 of the GDPR.

51 Article 12(5) of the GDPR.

52 Article 12(6) of the GDPR.

53 Article 12(2) of the GDPR.

54 Article 12(5) of the GDPR.

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;[55] 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.[56]

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:

a the personal data are no longer necessary for the purposes for which they were collected;[57]

b the data subject withdraws consent to the processing and there is no other legal ground for the processing;[58]

c the data subject objects to the processing and there are no overriding legitimate grounds for the processing;[59]

d the personal data has been unlawfully processed;[60]

e 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;[61] and

f the personal data has been collected in connection with an online service offered to a child.[62]

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

a 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;

b where complying with a legal obligation which requires processing by Union or Member State law;

c reasons of public interest in the area of public health in accordance with Article 9(2)(h) and (i);

d for archiving purposes in the public interest, scientific, historical research or statistical research purposes;

e for the establishment, exercise or defence of legal claims;

f 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;[63]

55 Article 12(6) of the GDPR.
56 Article 12(2) of the GDPR.
57 Article 17(1)(a) of the GDPR.
58 Article 17(1)(b) of the GDPR.
59 Article 17(1)(c) of the GDPR.
60 Article 17(1)(d) of the GDPR.
61 Article 17(1)(e) of the GDPR.
62 Article 17(1)(f)) of the GDPR.
63 Article 12(5) of the GDPR.

g 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;[64] and

h 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.[65, 66]

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:

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

b the processing is unlawful and the data subject opposes the erasure of the personal data and requests 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;[67]

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;[68] 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.[69]

64 Article 12(6) of the GDPR.
65 Article 12(2) of the GDPR.
66 Article 17(3) of the GDPR.
67 Article 12(5) of the GDPR.
68 Article 12(6) of the GDPR.
69 Article 12(2) of the GDPR.

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 EDPB has 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'.[70]

In addition, the EDPB 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.[71]

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;[72]

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);[73] and

c the right is not restricted to data communicated by the data subject directly.[74]

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'.

---

70 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.

71 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.

72 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.

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 10.

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 3.

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;[75] 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.[76]

vi Company policies and practices

While the GDPR is not prescriptive as to the policies and procedures that a company should have in place, it emphasises the concept of accountability (i.e., the ability to demonstrate compliance with the GDPR). In turn, to comply with the accountability obligations under the GDPR, a company will need to have in place a number of policies and procedures. These may include, for example:

a a data protection policy – addressing how the company complies with the principles of the GDPR;

b a data processing record – to comply with Article 30 of the GDPR;

c legitimate interest assessments – where processing personal data relies on the legitimate interest ground for processing;

d data protection or fair processing notices – to comply with Articles 13/14 of the GDPR (e.g., for customers and employees);

e data processing provisions for inclusion in contracts entered into between controllers and processors – to comply with Article 28 of the GDPR;

f a vendor data protection questionnaire – to assess data protection compliance of processors processing personal data on company's behalf;

g a GDPR-compliant form of consent or checklist to assess requirements for valid consent;

h data treatment guidelines – to address how in practice the company complies with the data treatment principles under Article 5 of the GDPR;

i a data protection impact assessment template and guidelines for when it should be completed;

j a records retention policy and schedule – which will in fact be broader than data protection;

k information security policies and procedures, and a personal data breach response plan;

l data subject rights' guidelines – addressing how in practice the company will respond to a request made by a data subject to exercise their rights under the GDPR;

m EU standard contractual clauses or other data transfer solutions;

n a data protection officer (DPO) assessment – to document whether or not the company is under a statutory obligation to appoint a DPO;

o a GDPR audit checklist;

p a data protection representative agreement – as required under Article 27 of the GDPR;

75 Article 21(1) of the GDPR.

76 Article 21(6) of the GDPR.

q a lead DPA assessment – documenting whether or not the company can take the benefit of the one-stop-shop principle under the GDPR and in turn, identify a lead DPA and if so, which DPA will likely be the lead DPA; and
r GDPR training materials for staff.

vii 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 EDPB 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 the purpose of the processing and a range of other factors, including, for example, whether the processing causes, or is likely to cause, damage, loss or distress to data subjects; or
d whether it 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.[77]

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

77 Article 4(16) of the GDPR.

EU, the main establishment will be where its main processing activities are undertaken. The EDPB in its guidance on lead supervisory authorities, make it clear that the GDPR does not permit 'forum shopping'[78] 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.[79]

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:

a the establishment of the controller or processor subject to the investigation is in the concerned DSA's Member State;

b 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

c a complaint has been lodged with that DSA.[80]

In the case of a dispute between DSAs, the EDPB shall adopt a final binding decision.[81] 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.[82]

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.

Since the coming into force of the GDPR, the EDPB has been fairly active in publishing GDPR guidance and for the most part this has been well received by companies. In addition to the GDPR guidance published by the former Article 29 Working Party and adopted by the EDPB, the EDPB has finalised guidelines on codes of conduct and certification mechanisms. The EDPB has also published a variety of draft guidelines including addressing the territorial scope of the GDPR and video surveillance. We expect to see further guidance published in the coming year.

Enforcement rights

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

a 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

78 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.

79 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 10.

80 Article 4(22) of the GDPR.

81 Article 65(1) of the GDPR.

82 Article 60 of the GDPR.

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.

b 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.

c 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.[83]

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.[84] 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.

83 Article 83(4) of the GDPR.

84 Article 83(5) of the GDPR.

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 corrective[85] and authorisation and advisory[86] powers.

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:

a issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of the GDPR;

b issue reprimands to a controller or processor where processing operations have infringed provisions of the GDPR;

c 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;

d 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;

e order the controller to communicate a personal data breach to the data subject;

f impose a temporary or definitive limitation on processing, including a ban;

g 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

h 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:

a 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;

b authorise processing pursuant to Article 36(5) of the GDPR, if the law of the Member State requires prior authorisation;

c issue an opinion and approve draft codes of conduct pursuant to Article 40(5) of the GDPR;

d issue certifications and approve criteria of certification in accordance with Article 42(5) of the GDPR; and

e approve binding corporate rules pursuant to Article 47 of the GDPR.

85 Article 58(2) of the GDPR.

86 Article 58(3) of the GDPR.

vii 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'.[87]

The GDPR also states health data should include the following:

a 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;

b information collected in the course of registration for or the provision of healthcare services;

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.[88]

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[89] 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

87 Article 4(15) of the GDPR.

88 Recital 35 of the GDPR.

89 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.

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).[90]

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.[91] The ePrivacy Directive was also amended in 2009[92] 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 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.[93]

The former Article 29 Working Party published an opinion on the cookie consent exemption[94] 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.[95]

In July 2016, the former Article 29 Working Party issued an opinion on a revision of the rules contained in the ePrivacy Directive.[96]

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.[97] The ePrivacy Regulation will complement the GDPR 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:

a require a clear affirmative action to consent to cookies;

b attempt to encourage the shifting of the burden of obtaining consent for cookie use to website browsers; and

c 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.

90 Article 13(3) of the ePrivacy Directive.

91 Recital 20 and Article 4 of the ePrivacy Directive.

92 Directive 2009/56/EC.

93 Article 5(3) of the ePrivacy Directive.

94 WP 194 – Opinion 04/2012 on Cookie Consent Exemption.

95 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.

96 Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC).

97 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 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 2021 at the earliest.

IV CLOUD COMPUTING

In its guidance on cloud computing adopted on 1 July 2012,[98] 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 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 Directive should be read as references to the GDPR.

i Instructions of the controller

To comply with the requirements of the 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[99]

Under the 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[100]

Under the Directive, a 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 of the cloud

98 WP 196 – Opinion 5/2012 on Cloud Computing.

99 Article 6(b) of the Data Protection Directive.

100 Article 17(2) of the Data Protection Directive.

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[101]

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[102]

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[103]

As discussed above, under the 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.

101 Article 6(e) of Data Protection Directive.

102 Article 12 and 14 of the Data Protection Directive.

103 Article 25 and 26 of the 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 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[104] providing various recommendations under the now repealed 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 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.

104 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.

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 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 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:

a the entity responsible for the ethics reporting programme;
b 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 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 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 former Article 29 Working Party published a working document providing guidance to controllers in dealing with requests to transfer personal data to other jurisdictions outside the EEA for use in civil litigation[105] 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 pre-trial e-discovery procedure include consent of the data subject and compliance with a legal obligation. However, the former Article 29 Working Party 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 and was effectively replaced on 12 July 2016 by the Privacy Shield. In the absence of any updates from the EDPB to the former Article 29 Working Party's 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.[106] As

105 WP 158 – Working Document 1/2009 on pretrial discovery for cross-border civil litigation adopted on 11 February 2009.

106 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 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:

a 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;

b the transfer is necessary for the performance of a contract between the data subject and the controller;

c the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject;

d 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;

e the transfer is necessary for the establishment, exercise or defence of legal claims;

f 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

g 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.[107]

VII EU CYBERSECURITY STRATEGY

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.[108]

The main elements of the NIS Directive include:

a new requirements for 'operators of essential service' and 'digital service providers';

b a new national strategy;

c designation of a national competent authority; and

d designation of computer security incident response teams (CSIRTs) and a cooperation network.

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.[109] This includes having research and development plans in place or a risk assessment

107 Article 49 of the GDPR.

108 Directive (EU) 2016/1148 of the European Parliament and the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

109 Article 7 of the NIS Directive.

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,[110] and setting up of at least one CSIRT that is responsible for handling risks and incidents.[111]

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.[112] 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[113] 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.[114] 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:

a the number of users affected;
b the dependency of other key market operators on the service provided by the entity;
c the duration of the incident;
d the geographic spread of the area affected by the incident;
e the market share of the entity; and
f 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.

Organisations should review the provisions of the NIS Directive and of any relevant Member State implementing legislation and take steps as applicable to amend their cybersecurity practices and procedures to ensure compliance.

110 Article 8 of the NIS Directive.
111 Article 9 of the NIS Directive.
112 Article 11 of the NIS Directive.
113 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.
114 Article 14 of the proposed NIS Directive.

iv New Cybersecurity Act

In June 2019, the EU Cybersecurity Act[115] (Act) came into force. The Act creates 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 introduces 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 Act is part of the European Union's push towards a digital single market.

The Act includes a permanent mandate for ENISA as the renamed European Union Agency for Cybersecurity and grants ENISA 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 will 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 will allow certificates to be issued by ENISA ensuring an adequate level of cybersecurity for the ICT products and services, which will 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.

On 26 June 2019, the European Commission released questions and answers on EU cybersecurity that address the certification framework among other things.

VIII OUTLOOK

The GDPR came into force over a year ago and while it appears the immediate panic surrounding it seems to have subsided, the legislation remains a hot topic and one many companies continue to grapple with. The GDPR continues to evolve with new guidance being published at an EU and national level. At the same time there have been a number of enforcement actions and cases dealing with the requirements of the GDPR that companies will need to carefully consider. Dealing with the GDPR has been made more difficult by the lack of consistency in approach taken at a national level by EU Member States and this remains the case in spite of guidance being published by the EDPB at an EU-level.

Many companies are now undertaking a review of the work undertaken in the run-up to May 2018 to assess their GDPR compliance and to re-evaluate certain decisions (GDPR 2.0). International companies are also taking the one-year anniversary as an opportunity to review their broader privacy compliance programmes and so leveraging work undertaken as part of their initial GDPR project to address, for example, the California Consumer Privacy Act of 2018 (CCPA).

Data subjects in the EU have made use of the substantial data protection rights provided by the GDPR at a rapid pace. For example, an airline has been threatened with a £500 million class action lawsuit in a UK court for non-material damage caused by a security breach. The airline has already pledged to cover any losses suffered by its customers, but a law firm acting for some of the affected individuals has taken the position that under the GDPR, the individuals have a right to further compensation of £1,250 each. A steep increase

115 Regulation (EU) 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No. 526/2013.

in consumers exercising their privacy rights and a growth in privacy litigation is expected this year and the next. We also expect to see an increase in GDPR-related enforcement action as demonstrated by the recent announcements made by the UK's ICO of its intention to fine British Airways £183 million and Marriott £99 million for cyberbreaches.

A further 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 31 October 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 31 October 2019, the UK may become a third country and if so will face restrictions on any transfer and processing of personal data of EU data subjects from the EEA to the UK.

Chapter 3

APEC OVERVIEW

Ellyce R Cooper, Alan Charles Raul and Sheri Porath Rockwell[1]

I OVERVIEW

The Asia-Pacific Economic Cooperation (APEC) is a regional economic forum established in 1989 to enhance economic growth and prosperity in the region. It began with 12 Asia-Pacific economies as an informal ministerial-level dialogue group, and has grown to include the following 21 economies as of July 2019: 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.[2] 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.' Collectively, APEC's 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.[3]

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. Towards that end, 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 1999, 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), which began to work towards the development of consistent legal, regulatory and policy environments in the Asia-Pacific

1 Ellyce R Cooper and Alan Charles Raul are partners and Sheri Porath Rockwell is an associate at Sidley Austin LLP. The current authors wish to thank Catherine Valerio Barrad, who was the lead author for the original version of this chapter and made substantial contributions to prior updates. She was formerly a partner at Sidley and is now university counsel for San Diego State University.

2 The current list of APEC member economies can be found at www.apec.org/About-Us/About-APEC/Member-Economies.

3 See www.apec.org/FAQ.

area.[4] Soon thereafter, in 2003, APEC established the Data Privacy Subgroup under the ECSG to address privacy and other issues identified in the 1998 APEC Blueprint for Action on Economic Commerce.[5]

The work of the Data Privacy Subgroup led to the creation and implementation, in 2005, of the APEC Privacy Framework. 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. While 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.

4 The ECSG was originally established as an APEC senior officials' special task force, but in 2007 was realigned to the Committee on Trade and Investment. This realignment underscores the focus within the ECSG, and its Data Privacy Subgroup, on trade and investment issues.

5 APEC endorsed the Blueprint in 1998 to 'develop and implement technologies and policies, which build trust and confidence in safe, secure and reliable communication, information and delivery systems, and which address issues including privacy'. See APEC Privacy Framework (2005), Paragraph 1 (available at https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015)).

Thus, APEC's 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 adopting 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.[6] 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.[7]

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,

6 https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group.

7 https://www.apec2018png.org/media/press-releases/revise-framework-conducive-for-e-commerce-environment.

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 pertain to personal information about living individuals and do not apply to publicly available information or information an individual collects or uses in connection with their personal, family or household affairs. The principles apply to persons, businesses and organisations in the public and private sectors (referred to hereafter collectively as 'organisations') that control the collection, holding, processing or use of personal information. They do not apply directly to organisations that only act as agents or on behalf of others.

The APEC principles are based on the OECD Guidelines, but 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 permit a broader scope of exceptions and are slightly stronger than the OECD Guidelines with respect to notice requirements. In general, the APEC principles reflect the goals of promoting economic development and respecting the different legal and social values held by 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 is designed to make sure that individuals know what information is collected about them and for what purpose it is being used. It requires that organisations take reasonably practicable steps to provide notice either before or at the time personal information is collected. Notice is not required for the collection or use of publicly available information.

Principle III – collection limitation

This principle limits the collection of personal information to only that which is relevant to the purpose of collection. It also stresses that, where appropriate, information should be collected with notice to, or consent of, the data subject.

8 See APEC Privacy Framework (2015), Paragraph 18.

9 See APEC Privacy Framework (2015), Paragraph 17.

10 See APEC Privacy Framework (2015), Paragraph 5.

Principle IV – uses of personal information

This principle limits the use of personal information to only those uses that fulfil the purpose of collection and other compatible or related purposes. If information is collected with the consent of the data subject, is necessary to provide a service or product requested by the data subject, or is required by law, limiting the use of information to the purposes for which it was originally collected does not apply.

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 provides that individuals have the right to access their personal information, which includes the right to obtain the information within a reasonable time of the request and in a form that is generally understandable. Individuals may also challenge the accuracy of their personal information 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 the privacy rights of other individuals 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 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 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 body, 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'.[11] 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.[12] 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.[13]

iii Data privacy individual action plans (IAPs)

Data privacy IAPs are periodic, national reports to APEC on each member economy's progress in adopting the Privacy Framework domestically. IAPs are the mechanism of accountability by member economies to each other for implementation of the APEC Privacy Framework.[14] The IAPs are periodically updated as the Privacy Framework is implemented within each such economy. As of 2019, 14 member economies have IAPs.[15]

II 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.[16] 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

11 See APEC Privacy Framework (2015), Paragraph 37.

12 See APEC Privacy Framework (2015), Paragraphs 53, 37.

13 See APEC Privacy Framework (2015), Paragraphs 57–64.

14 See APEC Privacy Framework (2015), Paragraph 55.

15 See https://www.apec.org/Groups/Committeee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group.

16 See APEC Privacy Framework (2005), Paragraphs 46–48.

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.[17]

ii 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 2019, eight APEC economies participate in the CBPR system – Canada, Japan, Mexico, South Korea, Singapore, the United States, and the two most recent additions, Australia and Taiwan – with more expected to join.[18] The CBPR 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 its goals is to 'lift the overall standard of privacy protection throughout the [Asia-Pacific] region' through voluntary, enforceable standards set out within it.[19]

In general, the CBPR system requires organisations to adopt policies and procedures regarding the transfer of personal data across borders that meet or exceed the standards in the APEC Privacy Framework. Organisations that seek to participate in the CBPR system must have their privacy practices and policies evaluated by an APEC-recognised accountability agent to assess compliance with the programme. If the organisation is certified, its privacy practices and policies will then become subject to enforcement by an accountability agent or 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] CBPR's website (cbprs.org) includes general information about the system, charters and protocols, lists of current participants and certified entities, submissions and findings reports and template forms.[22]

Member economies' participation in the CBPR system

Member economies must be certified to participate in the CBPR system before any private organisations subject to their jurisdiction can participate in the programme.[23] The CBPR certification requirements for APEC member economies are as follows:

a participation in the APEC CPEA with at least one privacy enforcement authority;

17 See Sections III.ii and III.iii.

18 http://cbprs.org/about-cbprs/.

19 See http://cbprs.org/government/.

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 APEC Cross-Border Privacy Rules System Policies, Rules and Guidelines, at http://cbprs.org/documents/.

22 See www.cbprs.org.

23 http://cbprs.org/business.

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
- submission of the APEC CBPR system programme requirements enforcement map.[24]

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.[25]

Accountability agents

The CBPR system uses third-party accountability agents to certify organisations as CBPR-compliant. 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.

All accountability agents must be approved by the Electronic Commerce Steering Group or ECSG. The approval process begins with the submission by the proposed agent of an application and supporting documentation to the relevant authorities in the supporting economy in which the proposed agent intends to operate. The relevant authority will provide a preliminary review of the organisation and, if the authority supports the application, it will forward it to the chairs of the ECSG, the ECSG's Data Privacy Subgroup, and the Joint Oversight Panel. The Joint Oversight Panel then considers the application and will vote, by simple majority, on whether to recommend that the organisation be recognised as an accountability agent.

The proposed agent must meet the CBPR's requirements for accountability agents, which 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 propriety procedures meet the baseline requirements of the CBPR system); and

d completing and signing the signature and contact information form.[26]

Additionally, no accountability agent may have an actual or potential conflict of interest, nor may it provide any other services to entities it has certified or that have applied for certification.

Following an application and review process by the Joint Oversight Panel, the accountability agent can be approved by the ECSG upon recommendation by the Panel. Any

24 http://cbprs.org/government/economies-requirements/.

25 http://cbprs.org/government/economies-requirements/.

26 See http://cbprs.org/accountability-agents/cbprs-requirements.

APEC member economy may review the recommendation of any proposed accountability agent and present objections, if any, to the ECSG. Once an application has been approved by the ECSG, the accountability agent is deemed 'recognised' and may begin to certify businesses. 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.

Accountability agents are responsible for conducting initial certifications of organisations that want to participate in the CBPR system, and are also tasked with monitoring continued compliance with the APEC CBPR system standards. Towards that end, CBPR-certified organisations must submit annual attestations of compliance to their designated accountability agent. Accountability agents are responsible for ensuring that any non-compliance is remedied in a timely fashion and reported, if necessary, to relevant enforcement authorities. Accountability agents must publish their certification standards and promptly report all newly certified entities, as well as any suspended or terminated entities, to the relevant privacy enforcement authorities and the CBPR Secretariat.[27]

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.[28] As of July 2019, the CBPR system recognises three accountability agents: TRUSTe, Schellman & Company, and the Japan Institute for Promotion of Digital Economy and Community.[29] TRUSTe and Schellman are recognised to certify organisations subject to the jurisdiction of the United States Federal Trade Commission (FTC). The Japan Institute for Promotion of Digital Economy and Community (JIPDEC) is recognised to certify organisations under the jurisdiction of the Ministry of Economy, Trade and Industry of the government of Japan. Accountability agents for other countries have yet to be designated.

CBPR system compliance certification for organisations

If an organisation is subject to the laws of an economy that is certified to participate in the CBPR system and an accountability agent has been approved for that economy, the organisation may apply to be certified to transfer personal information between APEC economies. The process of becoming certified begins with the submission of a self-assessment questionnaire and relevant documentation to an APEC-recognised accountability agent. The accountability agent will then evaluate the organisation and determine whether it meets the criteria for CBPR certification. Organisations that are certified are listed on the CBPR website. As of July 2019, 29 organisations have been CBPR certified, 26 of which are based

27 http://cbprs.org/accountability-agents/ongoing-requirements/.

28 See http://cbprs.org/documents/.

29 http://cbprs.org/accountability-agents/.

in the United States with the remainder based in Japan.[30] Certified companies must undergo annual recertification, which the accountability agent reviews. The number of certified organisations is limited by the fact that economies other than the United States and Japan do not have accountability agents to service organisations in their economies.

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, 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, a mechanism by which data processors can be certified by an accountability agent.[31] The PRP programme does not change the fact that data controllers are responsible for processors' practices, and there is no requirement that data controllers engage only PRP-recognised processors.[32] The PRP certification, which is conducted by approved PRP accountability agents, is designed to assure that processing is, at a minimum, consistent with the data processing requirements that data controllers are required to observe under CBPR rules.[33]

The Joint Oversight Panel of the CBPR administers the PRP programme 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.[34] The rules governing certification of economies and accountability agents 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 pursuant to CBPR rules.[35]

As of July 2019, two APEC economies have joined the PRP system – the United States and Singapore and the only two PRP-certified accountability agents are from the United States.[36] Seven processors have been certified under the programme, all of which are based in the United States.[37]

30 A current list of APEC-certified organisations can be found at http://cbprs.org/compliance-directory/cbpr-system.

31 The PRP Purpose and Background Document can be found at http://cbprs.org/documents/.

32 APEC Privacy Recognition for Processors ('PRP') Purpose and Background, found at http://cbprs.org/documents/.

33 APEC Privacy Recognition for Processors ('PRP') Purpose and Background, found at http://cbprs.org/documents/.

34 APEC Privacy Recognition for Processors ('PRP') Purpose and Background, found at http://cbprs.org/documents/.

35 https://www.apec.org/~/media/.../APEC%20PRP%20Rules%20and%20Guidelines.pdf.

36 http://cbprs.org/documents/.

37 http://cbprs.org/compliance-directory/prp/.

iii The Cross-border Privacy Enforcement Arrangement (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.

Among other things, the CPEA promotes voluntary information sharing and enforcement by:

a facilitating information sharing among privacy enforcement authorities within APEC member economies;

b supporting effective cross-border cooperation between privacy enforcement authorities through enforcement matter referrals and parallel or joint enforcement actions; and

c encouraging cooperation and information sharing with enforcement authorities of non-APEC member economies.[38]

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 2019, CPEA participants included over two dozen Privacy Enforcement Authorities from 11 APEC economies.[39]

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.

III 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

38 https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx.

39 https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx.

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.[40] 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.

In February 2019, the EU released an extensive study on data protection certification mechanisms, which included a comparative analysis of the certification criteria under GDPR and APEC's CBPR system.[41] The study found that the CBPR system was a 'good example' of how to set up certification oversight mechanisms, yet concluded that the CBPR's data transfer rules and redress mechanisms did not correspond to GDPR certification standards.[42] It remains to be seen if interoperability arrangements between the two systems can be developed.

IV THE YEAR IN REVIEW AND OUTLOOK

The APEC CBPR system saw some growth in 2018–2019. In late 2018, Australia and Taiwan joined the APEC CBPR system.[43] In early 2019, Schellman & Company was certified as a CBPR and PRP accountability agent for the United States, joining TRUSTe. Between June 2018 and July 2019, seven additional companies have become CBPR certified, including large companies with significant international presence, such as Mastercard and General Electric.[44] Seven US-based companies received PRP certifications during the same time period, including Box, Inc, Mastercard and General Electric.[45]

Significantly, in September 2018, the CBPR system was endorsed as a valid mechanism to facilitate cross-border information transfers between the United States, Canada and Mexico in the United States–Mexico–Canada Agreement, the new trade agreement that was drafted to replace NAFTA.[46] The parties to the agreement, which as of July 2019 is still awaiting ratification, agreed to 'cooperate and maintain a dialogue on the promotion and

40 https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Data-Privacy-Subgroup-Meeting-with-European-Union.

41 https://ec.europa.eu/info/sites/info/files/data_protection_certification_mechanisms_study_publish_0.pdf.

42 Id. at 5.

43 http://cbprs.org/news/.

44 http://cbprs.org/compliance-directory/cbpr-system/.

45 http://cbprs.org/compliance-directory/prp/.

46 https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19_Digital_Trade.pdf.

development of mechanisms, including the APEC Cross-Border Privacy Rules, that further global interoperability of privacy regimes.'[47] It is hoped that this endorsement of the CBPR will elevate the stature of the programme and encourage other economies to join.

In the United States, the FTC remains active in preserving the integrity of the CBPR system by targeting companies that falsely represent compliance with CBPR. The FTC brought its first such enforcement action in 2016, against Very Incognito Technologies Inc.[48] 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 falsely represented that they participated in the APEC CBPR system.[49] In 2019, the FTC issued two warning letters against companies for making similar misrepresentations.[50]

The FTC has brought actions against other companies for similar misrepresentations in other trans-border programmes, such as the EU–US Privacy Shield programme.[51] The FTC's continued enforcement actions may signal that it intends to continue to play an active role in enforcement of cross-border data transfer certification programmes, including the CBPR.

47 https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19_Digital_Trade.pdf, at Art. 19.14(1)(b).

48 See In re Very Incognito Tech, Inc., FTC, No. 162 3034, final order, 21 June 2016.

49 www.ftc.gov/news-events/press-releases/2017/02/three-companies-settle-ftc-charges-they-deceived-consumers-about.

50 https://www.ftc.gov/news-events/press-releases/2019/06/ftc-takes-action-against-companies-falsely-claiming-compliance-eu.

51 In June 2019, the FTC approved a settlement with a company that falsely represented its compliance with the EU-US Privacy Shield programme, following its 2017 actions in approving settlements with three companies for similar misrepresentations. https://www.ftc.gov/system/files/documents/cases/182_3152_securtest_do.pdf; https://www.ftc.gov/news-events/press-releases/2017/11/ftc-gives-final-approval-settlements-companies-falsely-claimed.

Chapter 4

ARGENTINA

Adrián Furman and Francisco Zappa[1]

I OVERVIEW

Data protection was introduced to the Argentine legal system following the 1994 constitutional reform, with the incorporation of the habeas data procedure.[2] 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[3] 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.

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.

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.

---

1 Adrián Furman is a partner and Francisco Zappa is an associate at Bomchil. The authors wish to thank Catalina Malara, former associate at Bomchil, for her contribution to writing this chapter.

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.

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.

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. The draft bill (the Draft) was submitted to the legislative branch of government on 19 September 2018 and is yet to be treated by the respective chambers.

One of the main reasons for the executive branch to promote this change in legislation is the acknowledgement that technological advances have had a significant impact on privacy since the approval of the Data Protection Law, and therefore a new legislation is needed to protect individuals from new risks. Additionally, the recent international context (in particular, the enactment of the GDPR) has made it necessary for Argentina's legislation to adapt and update, especially if it intends to maintain international protection standards.

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 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:

5 Section 4 of the Draft.

6 Section 12 of the Draft.

7 Section 12 of the Draft.

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 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.

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.

Another relevant addition is the requirement for the creation of a data protection officer,[13] 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.[14]

Moreover, on 6 December 2018, Congress passed Law 27,483, which incorporated the Convention for the Protection of Individuals with regards to Automatic Processing of Personal Data into the local legal framework. The Committee of Ministers of the European Council had accepted Argentina's request to be invited to join the Convention in September 2017.

Continuing with its intention of updating and improving the data privacy framework, in January 2019 the Agency issued Disposition 4/2019 which established a set of best practice guidelines for the interpretation and application of the Data Protection Law. The Disposition provides guiding criteria on (1) right of access to personal data collected through closed circuit television cameras, (2) automated data processing, (3) data dissociation, (4) biometric data, (5) consent and (6) consent of minors.

Lastly, in the context of the presidential elections to take place during the second semester of 2019, in May 2019 the Agency issued Disposition 86/2019, which set forth the guidelines for data treatment with electoral purposes. Among other matters, the guidelines state that personal data published on social media, forums or web platforms with easy or unrestricted access is also subject to the principles of the Data Protection Law. Therefore, those who handle this type of public data must inform, at least through a global notification or a publication on the internet, the purpose of the treatment, the person or entity responsible for the treatment, the data handler's address and the rights of the data owners.

III REGULATORY FRAMEWORK

i 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:

13 Section 43 of the Draft.

14 Section 49 of the Draft.

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.

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. The registration process is free and the information provided to the Agency must be updated periodically.

iii Data subject rights

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.

iv 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. Additionally, Disposition 4/2019 approved best practice guidelines for individuals to exercise the access right regarding data obtained through closed circuit television cameras.

v 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.

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.

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.

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,[17] 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'.[18]

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). The United Kingdom was included through Disposition 34/2019.

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.

17 See footnote 3.

18 Section 12 of the Data Protection Law.

Moreover, the Agency issued Disposition 159/18, which detailed the guidelines for companies to draft and implement binding corporate rules or `BCRs´, which regulate intra-group international transfers of personal data.

According to the Disposition, BCRs adopted following the aforementioned guidelines allow the free flow of personal data within companies of the same business group, even if some companies are located in countries that do not provide an adequate level of protection.

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.

As previously detailed above, Disposition 10/2015 requires companies to draft a manual for the operation of closed circuit television cameras, Disposition 18/2015 contains guidelines for drafting privacy policies for app developers and Disposition 159/18 contains guidelines for drafting BCRs.

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, 19 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 Federal Court of Appeals on Contentious Administrative Matters has recently issued a valuable decision related to the consent needed in order for an assignment of personal data to be valid.[19] The judgement took place by virtue of an action brought by a third party against Resolution No. 166-E/2016 of the Presidency of the Cabinet of Ministers, which approved an agreement allowing ANSES (the Agency in charge of social security matters) to provide the Secretariat of Public Communication with information about the citizens registered before it from time to time, in order for the Secretariat to communicate different issues.

The main discussion was if a person's e-mail and phone number could be assigned without the owner's consent. The first argument brought by the national government in favour of the assignment was that in this case the owner's consent was not needed based on an exception of the Data Protection Law that lists certain personal data that can be assigned without the owner's consent (name, ID, tax identification number, occupation, date of birth and domicile). The national government considered that such list was not an exhaustive list and, consequently, could be extended to include a person's email and phone number. The Court considered that said exception should be interpreted restrictively and confirmed that the list was indeed an exhaustive list.

Secondly, the national government argued that another exception of the Data Protection Law should apply to this matter, which exempts the obtainment of consent for assigning personal data that 'is collected for the exercise of the functions of the powers of the State or by virtue of a legal obligation'. Upon this discussion, the Court considered that, in order for that exception to apply, certain specific requirements must arise (for example, that the information is necessary for the national defence, public security or suppression of crimes purposes, or if it is collected by the security or intelligence community), which shall also be interpreted restrictively.

The Court concluded that it is necessary to obtain the owner's consent for the assignment of a person's email and phone number and resolved therefore that such data should not be included in the assignment to be performed by ANSES to the Secretariat of Public Communication.

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

19 Federal Court of Appeals on Contentious Administrative Matters, Docket No. 49,482/2016, 'Torres Abad, Carmen C/En JGM s/habeas data', 3 July 2018.

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 and the National Securities Commission regarding data security obligations for financial institutions and publicly listed companies, 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, Argentine entered into a memorandum of understanding on cooperation in cybersecurity, cybercrime and cyberdefence between 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.

Despite the lack of any specific regulation included in the Data Protection Law, it does set forth a generic obligation for the data handlers to adopt all technical and organisational measures needed to guarantee the security and confidentiality of the personal data. Registration of personal data in files, registers or banks that do not meet technical conditions of integrity and security is prohibited.

Based on this generic obligation, the Agency started an investigation regarding a security breach suffered by an email provider (made public by the company), which had exposed personal data of its users. During the investigation, the Agency's technical area determined that the company had not taken the technical measures needed to prevent data breaches and therefore sanctioned the company with a fine. The Agency's decision is not final and can be judicially challenged.

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 finally be 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 in the medium term. 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.

Chapter 5

AUSTRALIA

Michael Morris[1]

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.[2] 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.[3]

There is no general charter of human rights in Australia,[4] 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.

2 See in particular *Giller v. Procopets* [2008] VSCA 236.

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 2017–18[5] (the most recent report as at 9 August 2019), the OAIC received 2,947 privacy complaints and responded to 19,407 privacy enquiries in the year ending 30 June 2018. The Commissioner also initiated 21 investigations, worked on 15 assessments, conducted three digital health assessments and received 305 mandatory notifications under the Notifiable Data Breaches scheme from organisations.

Although there have been several significant enforcement actions (see Section VII), 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 organisations[8] and political representatives.[9] There is no general exemption for not-for-profit organisations.

There is a broad exemption[10] 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;

5 Available at https://www.oaic.gov.au/assets/about-us/our-corporate-information/annual-reports/oaic-annual-reports/annual-report-2017-18/oaic-annual-report-2017-18.pdf.

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 organisations to which 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,[12] 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.

12 'Guide to securing personal information: 'Reasonable steps' to protect personal information: January 2015', available at www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information.

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 Data subject rights

Individuals can request access to their personal information under APP 12 and entities must comply with such requests, subject to certain exceptions (for example, where giving access would pose a serious threat to the life, health or safety of any individual, or would have an unreasonable impact on the privacy of other individuals). Further, APP 13 provides that entities must take reasonable steps to correct personal information where the individual requests the entity to do so.

While individuals do not currently have an express legal right to require the removal or erasure of their personal information, entities have a general obligation to take reasonable steps to de-identify or destroy personal information where it is no longer needed for any purpose for which it may be lawfully used or disclosed by the entity under the APPs (see APP 11.2).

Individuals do not have a direct cause of action against entities to seek redress for breaches of the APPs (for further detail, see Section VII.iii). However, an individual may complain to the Commissioner who can make a determination that compensation be paid to the individual. This is explained in more detail in Section VII.

On 1 August 2019, legislation was passed to effect a 'consumer data right'. This will facilitate data portability for individuals across the banking industry initially. It is likely that this portability right will then be rolled out across other industries, such as the energy and telecommunications sectors. Currently, no express data portability right exists for individuals.

13 Section 7.11, Privacy Guidelines, 'Chapter 7: Australian Privacy Principle 7 – Direct marketing: Version 1.1, 22 July 2019' available at www.oaic.gov.au/images/documents/privacy/applying-privacy-law/app-guidelines/chapter-7-app-guidelines-v1.pdf.

v 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

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:

a the organisation reasonably believes that the overseas recipient is bound by a law similar to the APPs that the individual can enforce;

b the individual consents to the disclosure of the personal information in the particular manner prescribed by APP 8; or

c 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:

a the kinds of personal information that the organisation collects and holds;

b how the organisation collects and holds personal information;

c the purposes for which the organisation collects, holds, uses and discloses personal information;

d how an individual may access personal information about the individual that is held by the organisation and seek correction of the information;

e 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;

f whether the organisation is likely to disclose personal information to overseas recipients;

g 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

14 'Privacy management framework: enabling compliance and encouraging good practice', available at www.oaic.gov.au/resources/agencies-and-organisations/guides/privacy-management-framework.pdf.

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:

a 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]

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 link[17] – 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

15 Section 98 of the Privacy Act.

16 Section 5B(1A) of the Privacy Act.

17 Section 5B(2) of the Privacy Act.

18 Section 5B(3) of the Privacy Act.

19 Section B.14, Privacy Guidelines, available at www.oaic.gov.au/images/documents/privacy/applying-privacy-law/app-guidelines/APP-guidelines-combined-set-v1.pdf.

20 Section 13D(1) of the Privacy Act.

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.

X OUTLOOK

On 23 August 2019, the OAIC released its Corporate Plan 2019–2020.[21] The Corporate Plan indicates that the OAIC's strategic priorities for the coming year are as follows: advancing online privacy protections for Australians; upholding privacy and information access rights frameworks (including by supporting the implementation of the consumer data right); and supporting the proactive release of government-held information.

More broadly, it seems likely that privacy regulation in Australia will be strengthened in the coming years. Although draft legislation has not yet been introduced, the federal government has proposed amendments to the Privacy Act, including:

a the increase of penalties for serious or repeated interferences with privacy to the greater of A$10 million, three times the value of any benefit gained by the entity through misusing personal information, or 10 per cent of the entity's annual domestic turnover; and

b the granting of new powers to the Commissioner to allow the latter to issue infringement notices of up to A$63,0000 where entities fail to cooperate with efforts to resolve minor breaches (this would not require a court application).

Further, the Australian Competition and Consumer Competition has also recently released a number of recommendations relating to privacy in Australia as part of its Digital Platforms Inquiry. Such recommendations include requiring consent for secondary uses of information, the introduction of strengthened notification requirements, and the introduction of protections for de-identified data.

In addition, the introduction of the EU's General Data Protection Regulation (GDPR) means that an additional layer of privacy regulation applies to many Australian entities. This is because the GDPR has extraterritorial effect; Australian entities that offer goods or services to individuals in the EU, or monitor individuals in the EU, may be bound by the GDPR.

21 Available at https://www.oaic.gov.au/assets/about-us/our-corporate-information/corporate-plans/corporate-plan-2019-20/corporate-plan-2019-20.pdf.

Chapter 6

BELGIUM

Steven De Schrijver and Olivier Van Fraeyenhoven[1]

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

b the Act of 28 November 2000 on Cybercrime;

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

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

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

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

g the Act of 30 July 2018 on the Protection of Natural Persons with regard to the Processing of Personal Data (the Data Protection Act)(which replaced 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; and

h the Act of 7 April 2019 establishing a framework for the security of networks and information systems of general Interest for public security.

Cybersecurity has increasingly received attention in Belgium in recent years, because of an increasing number of cybersecurity attacks on Belgian companies. The Cyber Readiness Report 2019 noted that around 70 per cent of the Belgian companies became a victim of one or more cyberattacks in 2018, resulting in an average loss of €329,000 per company. About 10 to 20 per cent of Belgian companies have taken out insurance against cybercrime.

Despite its substantial efforts to enhance cybersecurity, Belgium has risen to the 33rd most exposed country of 187 countries in Rapid7's National Exposure Index in 2018. 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 €4.5 billion every year.

1 Steven De Schrijver and Olivier Van Fraeyenhoven are partners at Astrea.

Cybercrime, including ransomware, is increasingly challenging companies in Belgium. The Belgian Federal Cyber Emergency Team notes up to 35 cases a day. In extreme cases, a large cyberattack can lead to a (partial) shutdown of a company. For instance, in July 2019, 150 out of 1,000 employees of an enterprise specialised in producing aircraft parts were technically jobless for almost a month following a ransomware attack.

Apart from more updates on cybersecurity, including the final implementation of the EU's Network and Information Security Act Directive (NIS Directive) into Belgian law, this contribution will set out the most important Belgian laws relating to privacy and data protection. It will look into the Belgian implementation of the GDPR and its first results.

II THE YEAR IN REVIEW

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 had come under fire by the Belgian Privacy Commission (renamed the Data Protection Authority (DPA) on 25 May 2018) in 2015. The Brussels Court of first instance concluded in its judgment of 16 February 2018 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. Consequently, 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 to delete all data it obtained unlawfully. Facebook lodged an appeal against this judgment with the Brussels Court of Appeal, which decided on 8 May 2019 to refer the case to the European Court of Justice. Given that the GDPR foresees a new cooperation-mechanism whereby only one DPA is competent to investigate a case, the European Court will have to determine whether the Belgian DPA can continue to work on the case, or whether the European Data Protection Board, or the Irish DPA - as Facebook's HQ is located in Ireland -, will become competent.

In February, the Belgian Supreme Court rendered its judgment determining whether Skype, as a foreign peer-to-peer internet software provider, should be considered as an electronic communications service provider under Belgian law and therefore whether it should be subject to the jurisdiction of the Belgian courts. In 2016, the Court of First Instance of Mechelen ruled that Skype's duty to cooperate with the Belgian judicial authorities was not only limited to disclose certain information, but also to provide technical assistance for the interception of the content of 'live' voice communications. In an earlier case concerning Yahoo! it was possible to locate the obligation to disclose information (and thus jurisdiction) in Belgium on the grounds of the 'portability' of information, despite the fact that Yahoo! lacked any establishment or personnel in Belgium. By contrast, Skype is a Luxembourg company without infrastructure in Belgium, which would require material acts abroad to be made by the Belgian judicial authorities to request disclosure of information.

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.

This judgment was confirmed by the Court of Appeal of Antwerp. In the end, the Belgian Supreme Court has upheld the former judgement. The Court did not submit a question for a preliminary ruling to the European Court of Justice, as requested by Skype, that sought to argue that the need for an establishment in a certain Member State to provide wiretapped communications to the national authorities may violate the freedom to provide services (art. 56 of the Treaty on the Functioning of the European Union). The Court explained that an electronic communications service provider does not need any establishment in Belgium, but has to technically organise himself in such a way to make it possible to deliver wiretapped conversations to the Belgian authorities, be it digitally. Amongst others, the Court emphasised that Skype had been fined for not cooperating with the Belgian authorities, but not for lacking any technical infrastructure in Belgium.

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 Act 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 leaned closely towards those used in EU law, but had to 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 requirements under the Data Protection Act.

Belgium has also established an Information Security Committee that is competent to preventively control whether the communication of personal data within the government, via the Crossroads Bank for Social Security, or of health data, complies with the GDPR's basic principles. It can also grant deliberations that will be binding between the parties and on third parties.

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 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.

ii 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;

g 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;

h is necessary for medical reasons;

i 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

j is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes based on law 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.

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 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.

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.

Another obligation under the GDPR is 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 Data subject rights

The GDPR sets out clearly which rights data subjects possess. In particular, data subjects have:

a the right to certain information when personal data are collected from the data subject (Article 13) or have not been obtained from him or her (Article 14), such as the identity of the controller, the period for which the personal data is stored or the possibility to access, rectify or erase the personal data held by the controller;

b the right of access (Article 15), whereby the data subject can inquire whether his or her personal data are being processed or not, and whereby, where that is the case, he or she can access the personal data and information such as the purpose of the processing, the recipients of the personal data or the source of the personal data;

c the right to rectification (Article 16), by which inaccurate personal data can be rectified;

d the right to erasure ('the right to be forgotten') (Article 17), which sets out certain grounds which can apply to exercise the right to obtain from the controller the erasure of personal data concerning him or her;

e the right to restriction of processing (Article 18), based on, for instance, an unlawful processing of personal data;

f the right to data portability (Article 20), which facilitates the transfer of personal data held by a certain controller to another;
g the right to object (Article 21) the processing of personal data;
h the right not to be subject to a decision based solely on automated processing, including profiling (Article 22).

iv 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.
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.

On 3 May 2019, the Belgian Network and Information Security Act (the NIS Act) entered into force, finally transposing the EU Network and Information Security Directive (the NIS Directive) into Belgian law, nearly a year too late as this should have been done by the EU Member States by 25 May 2018 together with the entry into force of the GDPR. In addition to the specific data protection rules above, the NIS Act adds a legal basis for higher cybersecurity standards in respect of certain 'essential' services.

Following the Act, authorised government entities on two different levels, with separate functions, will be in charge of the compliance with the NIS Act. 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;
d health and drinking water supply and distribution; and
e digital infrastructure (including digital services such as online sales platforms, online search engines and cloud computing services).

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 Act sets out the following obligations for these OESs:

a 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
b 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 Act should increase transparency regarding network and information security and heighten awareness of cybersecurity risks in the above-mentioned essential services.

The 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 (e.g. fines).

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.

v Technological innovation and privacy law

Big-data analytics

The Belgian DPA's most recent report on big data dates from March 2017. It 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. It provides for 33 concrete recommendations on how to apply data protection principles to big data, covering 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 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 ePrivacy 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 remain in 'trilogue' negotiations since to determine the final text. The latest draft text was published on 12 July 2019 by the European Council. 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 ePrivacy Regulation would enter into force simultaneously with the GDPR, but the negotiations have been delayed and it is currently unknown when an agreement on the final text will be reached.

Electronic marketing

Electronic marketing and advertising is regulated by the provisions of Book XII (Law of the Electronic Economy) of the Code of Economic Law, which has transposed Directive 2002/58/EC of the European Parliament and the Council of 12 July 2002, as adopted by the Act of 15 December 2013, as well as the Royal Decree of 4 April 2003 providing for exceptions.

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 ePrivacy 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.

The European Data Protection Board (EDPB) issued its Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR underlining the necessity of both pieces of legislation. In some cases, both apply, or the ePrivacy Directive even goes further than the GDPR (e.g., by protecting the legitimate interests of legal persons instead of only natural persons). So, if the ePrivacy Directice makes GDPR rules more specific, the former should prevail. In online marketing, for instance, if the ePrivacy Directive sets out a requirement to obtain consent for specific data processing, this will override all other possible lawful grounds for processing provided for by Article 6 of the GDPR.

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:

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

b 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 cameras 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 cameras are also used for one of the purposes listed 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:

a the protection of health and safety;

b the protection of the company's assets;

c control of the production process; and

d 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.

Electronic privacy issues

The Belgian broadcaster VRT made public in July 2019 that it had obtained access to more than 1,000 recordings of commands directed to Google assistants recorded by Google Home, Google Home Mini, or through a smartphone. While most of them were recorded when the assistant was started by giving the command 'Okay Google', more than 100 of the obtained recordings were made accidentally, following words that resembled the command. While the recordings are shared with contractors without any further details of the user, journalists were able to trace multiple users by the information shared in the recordings, including names or home addresses. Google has confirmed the practice, but claims that only 0.2 per cent of the recordings are being listened to by 'language experts' to improve its services. Following the revelation, Google announced that it would also not listen to recordings of Europeans for a period of three months. While users give permission to process those recordings in Google's terms and conditions, these do not mention that humans listen to them, nor for how long they are stored. Following the story in the media, the Belgian DPA has announced that it will probably launch an investigation into Google and has called on users to file complaints with the DPA.

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. The EU–US Privacy Shield survived the second annual review at the end of 2018, resulting in the appointment of an ombudsperson by the US in February 2019 to handle any EU citizens' complaints, the sole demand made by the EU following the review. Currently, the European Court of Justice is reviewing the *Schrems II* case, in which the international transfer of data by Facebook to the United States on the basis of standard contractual clauses has been challenged.

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 Data Protection Officer has become obligatory for many companies with the GDPR. The number of DPOs has grown from 989 to 4,397 within the first year following the entry into force of the GDPR, according to the Belgian DPA. Larger 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).

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 has been the subject of a heated debate before the Belgian Supreme Court and criminal courts in two major cases regarding Yahoo! and Skype (see above).

Belgian law enforcement makes frequent use of its powers to request data from providers of electronic communications services. For instance, Microsoft received 625 requests in 2018, Google 815 and Apple 449.

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.

Along with natural persons, legal persons, associations or institutions are also able to lodge a complaint of an alleged data protection infringement.

ii 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. As mentioned above, Facebook has been condemned by the Court of First Instance. Following the appeal filed by Facebook, the Brussels Court of Appeal has decided to refer the case to the European Court of Justice.

Within the first year of the functioning of the reformed DPA following the introduction of the GDPR on 25 May 2018 only one fine has been issued yet. The case involved a mayor who, in the execution of his powers as a public official, sent out an email to a few citizens shortly prior to the municipal elections in which he campaigned for himself. The DPA concluded that the mayor had abused personal data which he received during the exercise of his function for personal purposes and issued a fine of €2,000.

In July 2019, the DPA has reproached the Ministry of Health for not responding to a request of a citizen that wished to exercise his right of access following two complaints of the citizen concerned. No fine was issued, as, under Belgian law, a state institution cannot be fined for violating the GDPR. The fact that not all of the GDPR's provisions apply equally to state institutions has been criticised by the Federation of Enterprises in Belgium (FEB), which has started a case before the Constitutional Court against what it calls a 'discrimination of enterprises'.

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.

The Belgian DPA received 328 complaints following the entry into force of the GDPR, which mostly concerned data subject rights, camera surveillance or direct marketing. As mentioned above, only one fine has been issued until now.

Class actions were traditionally not possible under Belgian law until 1 September 2014, when a new Act on Class Actions entered into force. The Belgian consumer organisation Test-Aankoop, for instance, has launched a class action against Facebook together with sister-organisations in Spain, Italy and Portugal, demanding €200 damages per claim for abusing personal data of its users. In Belgium, 42,000 people have joined the class action, and in Europe overall 250,000 people.

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 before, according to the recent Supreme Court decision in the *Skype* case, 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. The NIS Act additionally provides 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 to the data subject can in some cases also be necessary, if there is a high risk to their 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. Within the first year following the entry into force of the GDPR, the DPA has been informed of the existence of 645 data breaches.

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 Cybersecurity 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

The GDPR has, as expected, not resulted in major changes to the Belgian situation in practice as Belgian legislation and the interpretation to it by the DPA have traditionally been in line with EU law, the positions of the European Commission and the Article 29 Working Party (now the European Data Protection Board). Although the GDPR has strengthened the investigative and sanctioning powers of the DPA, its effective functioning was impeded due to a delayed appointment of its new directors, which finally happened in April 2019. It is to be seen whether the DPA, now that it can fully function, will make more use of its newly acquired powers. Until now, it has only issued one fine, which, in comparison with the neighbouring countries, is extremely low. Apart from sanctioning, the DPA is still assisting companies, data controllers and data processors to comply with the GDPR.

Unfortunately, it is yet unsure when the ePrivacy Regulation, which will override the GDPR and provide for more clarity regarding specific issues that may arise concerning privacy in connection with online interactions, will be agreed upon. The ongoing negotiations only mean that its implementation will again be delayed until 2020 or later.

Chapter 7

CANADA

Shaun Brown[1]

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

Privacy breach notification requirements under the federal Personal Information Protection and Electronic Documents Act (PIPEDA) came into effect on 1 November 2018.[2] Private sector organisations subject to the law are now 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.[3]

In May, 2019, the government of Canada published a discussion document entitled 'Proposals to modernize the Personal Information Protection and Electronic Documents Act', which describes options, considerations and questions addressing such things as: providing consumers with more meaningful controls and transparency; data mobility rights; online reputation and de-Indexing; encouraging innovation with data trusts for enhanced data sharing; and enhancing oversight and enforcement. The government, which published this document as a follow up to the Standing Committee on Access to Information, Privacy

1 Shaun Brown is a partner at nNovation LLP.

2 SC 2000, c 5.

3 Guidance on data breach notification requirements can be found here: Office of the Privacy Commissioner of Canada, What you need to know about mandatory reporting of breaches of security safeguards, https://www.priv.gc.ca/en/privacy-topics/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/.

and Ethics (ETHI) review of PIPEDA completed in February 2018,[4] is still in the relatively early stages of considering PIPEDA amendments. It will likely be several years before any legislative amendments are made.

Finally, in June 2019, the Office of the Privacy Commissioner of Canada (OPC) published a consultation document on transborder data flows that, among other things, revisits a long-standing OPC Interpretation of PIPEDA that transfers of personal information to third-party organisations for 'processing' are not 'disclosures', and therefore not subject to consent requirements.[5]

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.[6]

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 Information[7] (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:

4 House of Commons Standing Committee on Access to Information, Privacy and Ethics, 'Towards Privacy by Design: Review of the personal information protection and electronic documents act' (Report) (Ottawa: February 2018), online: https://www.ourcommons.ca/DocumentViewer/en/42-1/ETHI/report-12/.

5 Office of the Privacy Commissioner of Canada, Consultation on transfers for processing – Reframed discussion document, 11 June 2019, https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-transfers-for-processing/.

6 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.

7 CAN/CSA-Q830-96; published March 1996; reaffirmed 2001.

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.

ii 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.[8]

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.[9]

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'.[10]

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.[11]

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:

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

8 *Dagg v. Canada (Minister of Finance)* [1997] 2 SCR, dissenting, 403 at Paragraph 68.

9 *Morgan v. Alta Flights Inc* (2006) FCA 121, affirming (2005) FC 421.

10 *Canada (Information Commissioner) v. Canada (Transportation Accident Investigation and Safety Board)*, 2006 FCA 157, Paragraph 34.

11 PIPEDA Case Summary #2009-010 – Report of Findings: Assistant Commissioner recommends Bell Canada inform customers about Deep Packet Inspection.

powerful means available for gathering and analysing 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'.[12]

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.

12 Office of the Privacy Commissioner of Canada, 'Policy Position on Online Behavioural Advertising', 6 June 2012, www.priv.gc.ca/en/privacy-topics/advertising-and-marketing/behaviouraltargeted-advertising/bg_ba_1206.

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.[13]

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.[14]

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

13 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.

14 This is often referred to as 'refusal to deal'.

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:

a the personal information is demonstrably non-sensitive in nature and context;

b 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;

c 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;

d 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

e 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.[15]

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;[16] 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.

15 Privacy Commissioner Canada, 'Interpretation Bulletin: Form of Consent', online: www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_07_consent.

16 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 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.

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.[17]

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.

17 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.

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:

a provide a full description of what information is collected, used and disclosed, and for what purposes;

b 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.[18] 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'.[19]

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.

18 Office of the Privacy Commissioner of Canada, 'Global Internet Sweep finds significant privacy policy shortcoming' (Ottawa: 13 August, 2013), online: www.priv.gc.ca/en/opc-news/news-and-announcements/2013/nr-c_130813.

19 Office of the Privacy Commissioner of Canada, 'Initial Results from our internet privacy sweep: the good, the bad, the ugly' (Ottawa: 13 August, 2013), online: http://blog.priv.gc.ca/index.php/2013/08/13/initial-results-from-our-internet-privacy-sweep-the-good-the-bad-and-the-ugly/.

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,[20] the Privacy Commissioner decided to address the issue by publishing its Policy Position on Online Behavioural Advertising (Policy Position).[21]

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;

20 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.

21 Office of the Privacy Commissioner of Canada, 'Policy Position on Online Behavioural Advertising', 6 June 2012, www.priv.gc.ca/en/privacy-topics/advertising-and-marketing/behaviouraltargeted-advertising/bg_ba_1206.

e information is limited to non-sensitive information, to the extent practicable;[22] and
f information is destroyed as soon as possible or effectively de-identified.

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,[23] wearable computing,[24] drones[25] and genetic information.[26]

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.

22 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 suffers 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.

23 Office of the Privacy Commissioner of Canada, 'Automated Facial Recognition in the Public and Private Sectors: Report prepared by the Research Group of the Office of the Privacy Commissioner of Canada', March 2013, www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2013/fr_201303.

24 Office of the Privacy Commissioner of Canada, 'Wearable Computing – Challenges and opportunities for privacy protection: Report prepared by the Research Group of the Office of the Privacy Commissioner of Canada', January 2014, www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2014/wc_201401.

25 Office of the Privacy Commissioner of Canada, 'Will the proliferation of domestic drone use in Canada raise new concerns for privacy?': Report prepared by the Research Group of the Office of the Privacy Commissioner of Canada, March 2013, www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2013/drones_201303.

26 Office of the Privacy Commissioner of Canada, 'Genetic Information, the Life and Health Insurance Industry and the Protection of Personal Information: Framing the Debate', December 2012, www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2012/gi_intro.

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.[27] 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.[28] 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.'[29]

The Privacy Commissioner has, since at least 2009, interpreted PIPEDA such that consent is not required for transfers to foreign jurisdictions, although organisations are required 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.[30] However, according to a recently published discussion document, the Privacy Commissioner is considering revising its interpretation of PIPEDA to require consent for transfers in some cases.[31]

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:

27 Subject to limited exceptions, public-sector bodies in British Columbia and Nova Scotia are required to ensure that personal information in their custody or control is only stored or accessed in Canada; see the Freedom of Information and Protection of Privacy Act, RSBC 1996, Chapter 165, s 30.1, and the Personal Information International Disclosure Protection Act, SNS 2006, c 3, s 5. These laws can pose challenges for service providers located outside Canada that seek to do business with public sector bodies in those jurisdictions.

28 Office of the Privacy Commissioner of Canada, Guidelines for Processing Personal Data Across Borders, January 2009, www.priv.gc.ca/media/1992/gl_dab_090127_e.pdf.

29 ibid.

30 ibid.

31 Office of the Privacy Commissioner of Canada, Consultation on transfers for processing – Reframed discussion document, 11 June 2019, https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-transfers-for-processing/.

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;[32] and

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.[33]

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.

32 Personal Information Protection Act, SA 2003, c P-6.5, s 6(1).

33 ibid., s 13.1(1).

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.[34] 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.

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,[35] the Department of Immigration and Citizenship Act,[36] and the Canadian Security Intelligence Service Act.[37]

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.

34 RSC, 1985, c 30.

35 SC 2000, c 17.

36 SC 1994, c 31.

37 RSC, 1985, c C-23.

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.[38]

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,[39] Manitoba,[40] Newfoundland and Labrador,[41] and Saskatchewan.[42] A common law tort for invasion of privacy was explicitly recognised for the first time in Ontario in 2012 in *Jones v. Tsige*.[43] The court awarded relatively modest damages at C$10,000 in that 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.[44] 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.[45] 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;[46]
b Bank of Nova Scotia;[47]
c Human Resources and Skills Development Canada;[48]
d Health Canada;[49]
e Durham Region Health;[50] and
f Rouge Valley Health System.[51]

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

38 *Chitrakar v. Bell TV*, 2013 FC 1103.
39 Privacy Act, RSBC 1996, c 373.
40 Privacy Act, RSM 1987, c P125.
41 Privacy Act, RSN 1990, c P-22.
42 Privacy Act, RSS 1978, c P-24.
43 2012 ONCA 32.
44 *Vanderveen v. Waterbridge Media*, 2017 ON SCSM 77435 (CanLii).
45 *Jane Doe 464533 v. ND*, 2016 ONSC 541.
46 No citations: *Knuth v. Home Depot*, Statement of Claim, QBC 2006-14, *Lozanski v. Home Depot*, Statement of Claim, CV-14-51262400CP.
47 *Evans v. The Bank of Nova Scotia*, 2014 ONSC 2135.
48 *Condon v. Canada*, 2014 FC 250.
49 *John Doe v. Her Majesty the Queen*, 2015 FC 916.
50 *Rowlands v. Durham Region Health, et al.,* 2012 ONSC 394.
51 No citations: *Elia Broutzas 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.

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.'[52] However, settlements may be much higher where plaintiffs can provide more specific evidence of harm resulting from a breach.[53]

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

Organisations that collect, use or disclose personal information about Canadians are likely subject to Canadian law, regardless of their location. The Federal Court of Canada most recently affirmed in 2017 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.[54]

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.

The Alberta Personal Information Protection Act was the first private sector law in Canada with an explicit requirement to notify individuals in the case of a security breach.[55] As of 1 November 2018, PIPEDA requires organisations 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 must consider the sensitivity of the information involved and the probability that the information will be misused. Any breach of safeguards if it is reasonable to believe in the circumstances that the breach poses a real risk of significant harm.[56] Failure to comply with the new notification requirements could result in a penalty of up to C$100,000.

52 *Lozanski v. The Home Depot, Inc.*, 2016 ONSC 5447, para. 100.

53 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.

54 *A.T. v. Globe24h.com*, 2017 FC 114 (CanLII).

55 See Personal Information Protection Act, SA 2003, Sections 34.1 and 37.1.

56 See Division 1.1 of PIPEDA.

X OUTLOOK

Organisations doing business in Canada should pay close attention to the Privacy Commissioner's evolving views on transborder data flows, as the Commissioner may begin Interpreting PIPEDA to require consent for at least some transfers of personal information to third-party data processors.

Also, while a relatively slow-moving process, it will be important to watch as the government moves to amend PIPEDA in ways that could make the law more closely aligned with the European Union General Data Protection Regulation in some respects.

Chapter 8

CHINA

Hongquan (Samuel) Yang[1]

I OVERVIEW

At present, there is no omnibus privacy and data protection law in China, with the current provisions on privacy and data protection mainly found in laws and the industry-specific regulations.

In 2012, the Standing Committee of the National People's Congress issued the Decision on Strengthening Internet Information Protection, which provides some general principles for network service providers to protect the personal electronic information of Chinese citizens. Based on these principles, various departments under the State Council issued administrative regulations regulating the collection and processing of personal information in their respective fields. For example, the Ministry of Industry and Information Technology (MIIT) issued the Provisions on Protecting the Personal Information of Telecommunications and Internet Users in 2013, the State Post Bureau released the Provisions on the Security Management of Personal Information of Users of Posting and Delivering Services in 2014, and the People's Bank of China released the Implementing Measures for the Protection of Financial Consumers' Rights and Interests in 2016.

On 7 November 2016, the Cybersecurity Law (CSL) was issued and it took effect on 1 June 2017. The official implementation of the CSL marks the gradual formation of China's new legal framework for cybersecurity and data protection. Among other things, the CSL covers the following aspects:

a personal information protection;
b general network protection obligations of the network operators and the multi-level protection scheme (MLPS);
c enhanced protection for the critical information infrastructure (CII);
d data localisation and security assessment for the cross-border transfer of personal information and important data; and
e security review of the network products and services.

As the CSL is a high-level law and does not provide practical guidelines, China has been drafting a series of related implementation regulations and national standards. These implementation regulations and national standards, together with the CSL, constitute China's legal regime for cybersecurity and data protection.

1 Hongquan (Samuel) Yang is a partner at AnJie Law Firm.

II THE YEAR IN REVIEW

Since its promulgation, the CSL has exerted great influence on China's cybersecurity and data protection practice. Recent notable changes include the following.

i Personal information protection:

On 1 May 2018, the Information Security Technology – Personal Information Security Specification (the Specification), a national standard took effect. Although the Specification is a recommended national standard, owing to the lack of a uniform personal information protection law, the Specification has, to some extent, been regarded as 'best practice' by enterprises. As the enforcement authorities also refer to the Specification in various personal information protection campaigns, the Specification has gained some authority.

In the internet and mobile applications field, China has launched a number of enforcement campaigns to punish the unlawful or unreasonable collection or misuse of personal information.

In January 2018, the Cyberspace Administration of China (CAC) interviewed the relevant officials of Alipay and Zhima Credit for what is known as the Alipay annual bill incident, and called for a special rectification in their personal information collection practice.

In January 2018, the MIIT, in response to the violation of the privacy of users by relevant mobile phone apps, interviewed Baidu, Alipay and Toutiao, requiring the three enterprises to rectify their practice and to protect the users' right to know and right to choose.

In November 2018, the China Consumers Association released the Assessment Report on Collection of Personal Information by 100 Apps and their Privacy Policies.

In January 2019, the CAC and a number of other ministries jointly released the Announcement on Launching Special Crackdown Campaign Against Illegal Collection and Use of Personal Information by Apps, publicly exposing and ordering rectification of these apps' illegal collection of personal information and lack of a privacy policy.

ii Cybersecurity and data leakage

After the official implementation of the CSL, a number of enterprises have been punished for their failure to perform network security protection obligations or for data leakage.

In May 2018, a company in Yunnan province was warned and fined by the public security authority for failing to take technical measures to prevent computer viruses and cyberattacks, network intrusions and other harmful behaviour.

In July 2018, Datatang, a well-known domestic data company, was investigated and found illegally selling a huge volume of citizens' personal information.

In August 2018, many residents of Huazhu, a domestic hotel, had their personal information leaked and sold online. The perpetrators were arrested.

iii Data localisation and cross-border transfer of data

In late 2018, the Ministry of Science and Technology published its penalties against BGI and Huashan Hospital for their international cooperation with Oxford University for research on Chinese human genetic resources without the approval of the competent authority. BGI was found to have transferred abroad information on human genetic resources over the internet. The two enterprises were ordered to stop the related study projects, destroy all the genetic materials and the related research data, and suspend any international cooperation on human genetic resources until they are reassessed as qualified again. It should be noted that the

punishment originated from the violation of the Provisional Administrative Measures of Human Genetic Resources, an industry-specific regulation effective long before the CSL was in place.

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

China's legal regime of privacy and data protection includes the CSL and privacy and data protection provisions dispersed in various laws and regulations, including:

a the National Security Law;
b the E-commerce Law;
c the Tourism Law;
d the Anti-Terrorism Law;
e the General Rules of the Civil Law;
f the Implementing Measures of the PRC for the Protection of Financial Consumers' rights and interests;
g the Interim Measures for the Administration of Online Taxi-Booking Business Operations and Services;
h the Criminal Law;
i the Administrative Provisions on Short Message Services;
j the Regulations on Management of Internet User Account Name;
k the Provisions on the Security Management of Personal Information of Users of Posting and Delivering Services;
l the Law on the Protection of Rights and Interests of Consumers;
m the Administrative Regulations on Credit Investigation Industry;
n the Several Provisions on Regulating the Order of the Internet Information Service Market;
o the Law on Resident Identity Cards;
p the Tort Law; and
q the Provisions on Protecting the Personal Information of Telecommunications and Internet Users;

China's legal regime on cybersecurity and data protection also includes the judicial interpretations made by the Supreme People's Court and the Supreme People's Procuratorate, such as:

a Interpretation of several issues regarding application of law to criminal cases of infringement of citizen's personal information handled by the Supreme People's Court and the Supreme People's Procuratorate; and
b Provisions of the Supreme People's Court on application of laws to cases involving civil disputes over infringement upon personal rights and interests by using information networks.

National standards are another key part of the cybersecurity and data protection legal regime. Though they are not compulsory, they are generally regarded as best practice by enterprises. Important national standards (including draft versions) include:

a Information Security Technology – Personal Information Security Specification;
b Information Security Technology – Guidelines for Personal Information Protection Within Information System for Public and Commercial Services;

c Information Security Technology – Guidelines for Data Cross-Border Transfer Security Assessment (Draft) (draft for comment);
d Information Security Technology – Guide to De-Identifying Personal Information (draft for comment);
e Information Security Technology – Security Impact Assessment Guide of Personal Information (draft for comment);
f Information Security Technology – Security Requirements for Data Exchange Service (Draft for Comment); and
g Information Security Technology – Risk Assessment Specification for Information Security (draft for comment); etc.

The CSL defines the terms 'network operator' and 'personal information'. Under the CSL, a network operator refers to the owner or manager of a network or the provider of a network service; personal information refers to various information that is recorded in electronic or any other form and used alone or in combination with other information to recognise the identity of a natural person, including but not limited to their name, date of birth, ID number, personal biological identification information, address and telephone number of the natural person.

The Specification makes minor wording changes to the definition of 'personal information' under the CSL. According to the Specification, personal information means any information saved in electronic form or otherwise that can be used independently or together with other information to identify a natural person or reflect the activities of a natural person, including names, dates of birth, identification numbers, personal biometric information, addresses, contact information, records and content of communications, accounts and the passwords thereof, property information, credit reference information, whereabouts and tracks, hotel accommodation information, information concerning health and physiology, information on transactions, etc.

The Specification also defines the 'personal sensitive information' as personal information that may cause harm to personal or property security, or is very likely to result in damage to an individual's personal reputation or physical or mental health or give rise to discriminatory treatment, once it is leaked, unlawfully provided or abused, including identification numbers, personal biometric information, bank accounts, records and content of communications, property information, credit reference information, whereabouts and tracks, hotel accommodation information, information concerning health and physiology, information of transactions, personal information of children aged 14 or younger, etc.

China has not had a specific stipulation on the ownership of personal information. It is still disputed on whether personal information belongs to the scope of property rights or personal rights or should be treated as a brand new type of legal right. A unified Personal Information Protection Law is being drafted by legislators and is expected to be issued in the near future, which may shed more light on the ownership of personal information.

The Specification also provides the definition of 'personal information subject' and 'personal information controller'. According to the Specification, a personal information subject means a natural person who can be identified by reference to personal information; a personal information controller means an organisation or an individual who has the right to determine the purposes and means of the processing of personal information. The Specification does not define the 'personal information processor'.

According to the Specification, the basic principles for personal information protection include:

a Consistency between rights and liabilities: it shall bear liabilities for any damage caused by its activities of processing personal information to the legal rights and interests of personal information subjects.

b Clear purpose: it shall have lawful, justified, necessary and clear purposes in processing personal information.

c Solicitation for consent: it shall explicitly specify the purposes, manners, scope and rules in respect of the processing of personal information, and seek their authority and consent.

d Minimum sufficiency: it shall merely process the minimum categories and amount of personal information necessary for achieving the purpose authorised and consented to by personal information subjects, unless otherwise agreed with personal information subjects. It shall delete the personal information in a timely manner as agreed once this purpose are achieved.

e Openness and transparency: it shall make public the scope, purposes, rules, etc. in respect of the processing of personal information in an explicit, easily understandable and reasonable manner, and accept public oversight.

f Guarantee of security: it shall be capable of ensuring security to a degree corresponding to the security risks it faces, and take sufficient management measures and technological approaches to safeguard the confidentiality, completeness and availability of personal information.

g Involvement of personal information subjects: it shall provide personal information subjects with opportunities to access, modify and delete their own personal information and to withdraw their consent and cancel their own account.

If in violation of the related provisions on personal information protection, according to Article 64 of the CSL, if network operators or providers of network products or services infringe upon any right in personal information that is legally protected, they will receive punishments from the competent authorities, such as ratification, warning, confiscation of illegal earnings and fines; if in severe violations, the punishment may cover suspension of related business, winding up for rectification, shutdown of their website, and revocation of their business licence. Also, stealing or otherwise unlawfully obtaining any personal information, or selling or unlawfully providing such information to others that does not constitute a crime will be punished through confiscation of the illegal earnings or a fine.

ii General obligations for data handlers

The CSL only provides some general principles for personal information protection, Article 41 of the CSL provides that:

> *Network operators shall abide by the 'lawful, justifiable and necessary' principles to collect and use personal information by announcing rules for collection and use, expressly notifying the purpose, methods and scope of such collection and use, and obtain the consent of the person whose personal information is to be collected. No network operator may collect any personal information that is not related to the services it provides. It shall collect and use, and process and store personal the information in the light of laws and administrative regulations and agreement with the users.*

As for the right of the personal information subject, Article 43 of the CSL provides that

> *Each individual is entitled to require a network operator to delete his or her personal information if he or she founds that collection and use of such information by such operator violate the laws, administrative regulations or the agreement by and between such operator and him or her; and is entitled to require any network operator to make corrections if he or she founds errors in such information collected and stored by such operator. Such operator shall take measures to delete the information or correct the error.*

The Specification provides more specific provisions on the collection and use of personal information.

Collection of personal information

Under the Specification, the collection of personal information should be subject to the principle of lawfulness, minimisation, as well as the authorisation of the personal information subject (explicit consent should be obtained if involving sensitive personal information). However, a personal information controller may collect and use personal information, without the need to obtain the authority and consent from personal information subjects, under any of the following circumstances,

a where the collection and use are in direct relation to state security or national defence security;

b where the collection and use are in direct relation to the public security, public sanitation, or major public benefits;

c where the collection and use are in direct relation to investigations into crimes, prosecutions, court trials, execution of rulings, etc.;

d where the collection and use are for the sake of safeguarding significant legal rights and interests, such as the life and property, of personal information subjects or other individuals, but it is difficult to obtain their consent;

e where the personal information collected is the information voluntarily published by personal information subjects before the general public;

f where the personal information is collected from information that has been legally and publicly disclosed, such as legal news reports and information published by the government;

g where the collection and use are necessary for inking and performing contracts as required by personal information subjects;

h where the collection and use are necessary for ensuring the safe and stable operation of its products or services, such as identifying and disposing of faults in its products or services;

i where the personal information controller is a news agency and the collection and use are necessary for releasing news reports in a legal manner;

j where the collection and use are necessary for the personal information controller, as an institute for academic research, to have statistical programmes or academic research for the sake of the general public, and it has processed the personal information, which is contained in the results of academic research or descriptions, for de-identification purposes, while announcing these results to the general public; or

k Other circumstances specified by laws and regulations.

The Specification specifies that explicit consent means the act of a personal information subject granting authority for the processing of his or her personal information, either through a written statement or his or her voluntary affirmative gesture, with the affirmative gestures including voluntarily making (either electronic or written) statements, or voluntarily ticking or clicking the 'agree', 'register', 'send', 'dial', or other options by personal information subjects.

Use of personal information

According to the Specification, a personal information controller is required to disable the ability of personal information it uses to clearly point to certain identities, unless as needed for realising certain purposes, to avoid a situation in which certain individuals are successfully identified; for newly generated information from the processing of the collected personal information that can identify natural persons' identities independently or together with other information or reflect their activities, such information should be treated as personal information; and not use personal information for any purpose beyond the scope directly or reasonably related to those purposes claimed by it at the time when the personal information is collected. Where it is truly necessary to use the personal information beyond the said scope to suit its business demands, it shall obtain explicit consent of personal information subjects concerned again.

If any circumstance below occurs, the personal information controller should notify the personal information subject.

a Prior to the collection of personal information. Personal information controller should inform personal information subjects explicitly of the categories of personal information that will be collected under different business functions of its products or services, and the rules on how personal information will be collected and used (for example, why, how and how often personal information will be collected and used, the territory where personal information will be stored, how long personal information will be stored, its data security capability, and particulars of its sharing, transferring and public disclosure of personal information), and obtain the authority and consent of personal information subjects.

b Suspension of personal information controllers' operation. If a personal information controller suspends operation in regard to its products or services, it shall serve a notice of suspended operation on each personal information subject or publicly release an announcement for this purpose.

c Sharing and transfer of personal information. The personal information controller shall inform personal information subjects of the purposes for which their personal information will be shared or transferred and categories of data recipients, and obtain the authority and consent of personal information subjects in advance. Before sharing or transferring personal sensitive information, it shall also inform what categories of personal sensitive information are involved, identities of data recipients and their data security capability, and shall obtain explicit consent of each personal information subject.

d Transfer of personal information in acquisitions, mergers and restructuring

e Public disclosure of personal information. The personal information controller shall inform personal information subjects of the purposes for which their personal information will be publicly disclosed and what categories of information will be

publicly disclosed, and obtain the authority and consent of personal information subjects in advance. Before publicly disclosing personal sensitive information, it shall also inform them of what personal sensitive information will be involved.

f Joint personal information controllers. The personal information controller shall determine and inform personal information subjects explicitly of, what requirements in respect of personal information security shall be fulfilled, and the respective duties and obligations of itself and the third party in respect of personal information security, in a contract or otherwise.

g Security incidents. A personal information controller is required to promptly notify each affected personal information subject of the particulars of the security incident, by means of emails, letters, calls or pushed notifications. Where it is difficult to notify all affected personal information subjects one by one, it shall issue alerts in relation to the general public in a reasonable and effective manner; the content of a notification shall include but not be limited to (1) what the security incident is and its impact; (2) what measures it has taken or will take to deal with the incident; (3) advice on what actions could be taken by personal information subjects themselves to avoid the impact and reduce risks; (4) remedial measures available for personal information subjects; and (5) contact information of the head in charge of personal information protection and the agency in charge of personal information protection.

iii Data subject rights

Article 43 of the CSL provides that

> *Each individual is entitled to require a network operator to delete his or her personal information if he or she founds that collection and use of such information by such operator violate the laws, administrative regulations or the agreement by and between such operator and him or her; and is entitled to require any network operator to make corrections if he or she founds errors in such information collected and stored by such operator. Such operator shall take measures to delete the information or correct the error.*

According to the Specification, the personal information subject has the right to access, modify, delete the personal information, withdraw the consent, cancel account, obtain the copies of personal information.

Access to personal information

A personal information controller shall provide personal information subjects with methods regarding how to access the following information,

a what personal information of the personal information subjects it holds, or categories of this personal information;

b from where the personal information is sourced, and for what; and

c the identities of third parties that have obtained the personal information, or categories of these third parties.

It should be noted that, where a personal information subject raises a request to access their personal information that is not voluntarily provided by itself, the personal information controller, may decide whether to agree to the request or not and give reasons, after

comprehensively taking into account the likely risks and damage that may arise to the personal information subject's legal rights and interests if it disagrees with his or her request, technical feasibility, costs of agreeing to the request, and other related factors.

Modification of personal information

If a personal information subject finds that his or her personal information held by a personal information controller is inaccurate or incomplete, the personal information controller shall make it possible for the subject to request correction of the information or the provision of additional information.

Deletion of personal information

A personal information controller is required to fulfil the requirements below:

a if a personal information subject requires it to delete their personal information under any of the following circumstances, it shall delete his or her personal information in a timely manner,
- where the personal information controller collects or uses the personal information in a way that violates the provisions of laws and regulations; or
- where the personal information controller collects or uses the personal information in a way that violates its agreement with the personal information subject;

b if it shares the personal information of a personal information subject with or transfers it to a third party, in violation of the provisions of laws and regulations or its agreement with the personal information subject, and the subject requires it to delete his or her personal information, it shall cease sharing or transferring the information immediately, and instruct the third party concerned to delete the information in a timely manner; and

c if it publicly discloses personal information in a way that violates the provisions of laws and regulations or its agreement with the personal information subject, and the personal information subject requires it to delete the information, it shall cease the public disclosure of the information immediately, and issue a notice to require related recipients to delete the information concerned.

Personal information subjects' withdrawal of consent

A personal information controller is required to make it possible for personal information controllers to withdraw their consent to the authorised collection and use of their personal information. Once the consent has been withdrawn, it shall no longer process the personal information concerned thereafter. A controller must also guarantee personal information controllers' rights to refuse to receive commercials pushed on the basis of their personal information. Where personal information is shared with, transferred or publicly disclosed to external parties, it shall make it possible for personal information subjects to withdraw their consent.

It should be noted that, a personal information subject's withdrawal of his or her consent does not affect the consent-based processing of personal information prior to the withdrawal.

Personal information subjects' cancellation of accounts

A personal information controller must meet the following requirements:

a if it offers services through registered accounts, it shall make it possible for personal information subjects to cancel their own account and the method to cancel an account should be easily and conveniently feasible; and

b after a personal information subject has cancelled his or her account, it shall delete or anonymise his or her personal information.

Personal information subjects' request for copies of personal information

A personal information controller shall, upon the request of a personal information subject, make it possible for the subject to obtain a copy of the following categories of his or her own personal information, or directly transit a copy of the following categories of his or her own personal information to a third party, provided that the technology is practicable:

a the subject's basic information and information about his or her identification; and

b the information about the subject's health, psychological status, education and employment.

iv Specific regulatory areas

Workplace privacy

There are no specific provisions in Chinese laws and regulations regarding workplace privacy protection. In the daily operation management, for the need of supervision and management, enterprises may monitor the behaviour of employees. It is generally considered that such monitoring behaviour falls under the enterprise's business autonomy scope, which has certain legitimacy. For example, companies may obtain images of employees through a camera, fingerprint of employees through attendance machines, or information about employees' location through app location function, which often involves collection of sensitive information of employees (whereabouts and tracks, biometric information, etc.). For the purpose of protecting the privacy of employees, enterprises should first ensure that the above-mentioned monitoring measures, as well as the employee information they collect, are for a legitimate purpose and are necessary for business operations, and avoid collecting or monitoring any employee information during non-working hours and outside the workplace. Second, the type, purpose, manner of collection and protective measures of the information collected should be notified to the employee, and the employee's written consent should be obtained.

Children's privacy

According to the Provisions on Cyber Protection of Personal Information of Children, 'network operators that collect, use, transfer or disclose personal information of children shall, in a notable and clear way, notify children's guardians of their practices, and obtain the consent from children's guardians.'

Health and medical privacy

The Measures for the Management of Population Health Information (on Trial), Law on Licensed Doctors of the PRC, Nurses Ordinance and the Regulations for Medical Institutions on Medical Records Management provide the requirements for medical institutions and staffs to protect patients' personal information. For example, the Regulations for Medical

Institutions on Medical Records Management require that, 'medical institutions and medical staff shall strictly protect patient privacy. Any leakage of patients' medical records for non-medical, non-teaching or non-research purposes is forbidden'.[2] It also provides the keeping, saving, borrowing and copying of the medical records.[3]

Financial privacy

The Notice of the People's Bank of China on Urging Banking Financial Institutions to Do a Good Job in Protecting Personal Financial Information and the Notice of the People's Bank of China on Issuing the Implementation Measures of the People's Bank of China for Protecting Financial Consumers' Rights and Interests provides the obligations that banking and financial institutions should fulfil. According to the two notices, personal financial information includes personal identity information, personal property information, personal account information, personal credit information, personal financial trading information, derivative information and other personal information obtained and preserved in the process of establishing a business in relation with a person. In protecting personal financial information, banking financial institutions should strictly abide by the legal provisions, establish and improve the internal control by-laws, improve the information security technology prevention measures, strengthen the training of the professionals and intensify professionals' awareness of personal financial information security. Provision of personal financial information collected inside China abroad is not allowed unless otherwise required by laws and regulations and the People's Bank of China.

v Technological innovation

For the use of cookies, the Guide to the Self-Assessment of Illegal Collection and Use of Personal Information by Apps provides that, 'For the collection of personal information by using cookies and similar technologies (including scripts, clickstreams, web beacon, flash cookie, embedded web links, SDK, etc.), the purposes and types of personal information collected shall be clearly presented to the users.'[4] For the use of cookies, generally companies will describe such use in the privacy policy, rather than setting up a separate pop-up on the webpage.

For profiling or automated decision-making, according to the Specification, 'personal information controller should specify in the privacy policy the purposes for which personal information will be collected and used, and what business functions are involved in these purposes, including using personal information in pushing commercials or creating direct user profiles and the use thereof.'[5] Besides, the Specification stipulates that, 'where a decision that has a dramatic impact on a personal information subject's rights and interests is made reliant only on the information system's automatic decision-making (for example, determining the subject's credit status and the quota of credit loans available to the subject,

2 Article 6 of the Regulations for Medical Institutions on Medical Records Management.

3 Article 16 of the Regulations for Medical Institutions on Medical Records Management.

4 Item 21, part 2 of the Guide to the Self-Assessment of Illegal Collection and Use of Personal Information by Apps.

5 5.6 of the Specification.

based on user profiling, or applying user profiling to shortlist candidates for interviews), the personal information controller shall make it possible for the personal information subject to lodge a complaint.'[6]

The CSL does not differentiate anonymisation, de-identification and pseudonymisation; it is noteworthy, however, Article 42 of the CSL provides that, 'No network operator may disclose, tamper with or destroy personal information that it has collected, or disclose such information to others without prior consent of the person whose personal information has been collected, unless such information has been processed to prevent specific person from being identified and such information from being restored.' Therefore, only when a technique, regardless of anonymisation, de-identification and pseudonymisation, could meet the requirement of 'such information has been processed to prevent specific person from being identified and such information from being restored', could the personal information processed not be regarded as personal information.

The Information Security Technology – Guide for De-Identifying Personal Information (Draft for Comment) provides the related requirements for de-identification, as well as the pseudonymisation technique.

The Specification regards the following personal information as personal sensitive information and requires the controller to obtain the personal information subject's explicit consent for the collection and process:

a information concerning property owned by an individual: bank account, identification information (code), deposit information (including the amount of deposits, records of receipts and payments, etc.), real estate information, credit loan records, credit reference information, records of transactions and consumptions, flow records, etc., and information about virtual property, such as virtual currency, virtual transactions, and CD-keys for games;

b information concerning the health and psychological status of an individual: records formed from an individual's illness and treatment, such as symptoms of illness, in-hospital logs, physician's advices, test reports, records of operations and anaesthesia, nursing records, records of drugs used, information on allergy to drugs and foods, childbirth information, his or her medical history, particulars of treatment, medical history of his or her family, history of present illness, history of infectious diseases, etc., and information generated from his or her physical conditions;

c biometric information of an individual: personal genes, fingerprints, vocal prints, palm prints, auricle, iris, facial features, etc.;

d identification information of an individual: identity card, military officer certificate, passport, driving licence, work licence, building pass, social insurance card, residence permit, etc.;

e information concerning online identification symbols: Account for a system, IP address, email address, and the password, code, answers to questions asked to protect the password and users' personal digital certifications for the said account or addresses, etc.; and

f other information: phone number, sexual orientation, marital history, religious belief, records of undisclosed violations and crimes, communication records and the content thereof, whereabouts and tracks, web-browsing history, information on hotel accommodation, information on accurate positioning, etc.

6 7.10 of the Specification.

Apart from obtaining explicit consent from the personal information subject, the current law in China does not impose any other restrictions on using the personal sensitive information. It is possible that the forthcoming personal information protection law will provide more details on those controversial personal information techniques (such as facial recognition technique).

IV INTERNATIONAL DATA TRANSFER AND DATA LOCALISATION

China has not yet concluded any international data protection framework or agreements.

Although the CSL provides the obligations for the CII operators to localise the personal information and important data collected and generated inside China, it does not elaborate on the definition and specific scope of the CII and the 'important data'; nor does it provide operational guidelines for the specific requirements of data localisation and security assessment for cross-border data transfer. The related implementation regulation and national standard is still in the progress of draft.

In May 2019, the CAC issued the Measures on Data Security Management (Draft for Comment) for public consultation, which provides that , 'Important data' refer to the kind of data, if divulged, may directly affect national security, economic security, social stability and public health and security, such as undisclosed government information, large-scale population, genetic health, geography and mineral resources, etc. Important data shall usually not include information related to the production and operation and internal management of enterprises or personal information, etc.'[7] and 'Network operators shall assess the potential security risks prior to releasing, sharing or selling important data or transferring such data abroad, and shall report to the competent regulatory department for approval. If the competent regulatory department is unclear, network operators shall report to the cyberspace administrations at the provincial level for approval.'[8]

In June 2019, the CAC issued the Measures for Security Assessment for Cross-border Transfer of Personal Information (Draft for Comment) for public consultation. It provides that, 'before the cross-border transfer of personal information, network operators shall apply to the local cyberspace administrations at the provincial level for security assessment for cross-border transfer of personal information.'[9] 'If it is identified by the security assessment that the cross-border transfer of personal information may affect national security or damage public interest, or that it is difficult to effectively protect the security of personal information, cross-border transfer of such information shall not be allowed.'[10]

According to the Measures on Data Security Management (Draft for Comment) and the Measures for Security Assessment for Cross-border Transfer of Personal Information (Draft for Comment), whether the important data and personal information can be transferred abroad should be decided by the government. Whether these controversial requirements will pass as they are remains to be seen.

7 Article 38 of the Measures on Data Security Management (Draft for Comment).

8 Article 28 of the Measures on Data Security Management (Draft for Comment).

9 Article 3 of the Measures for Security Assessment for Cross-border Transfer of Personal Information (Draft for Comment).

10 Article 2 of the Measures for Security Assessment for Cross-border Transfer of Personal Information (Draft for Comment).

As for the forensics of cross-border electronic data evidence, Article 4 of the Law on International Criminal Judicial Assistance provides that 'No foreign institution, organisation or individual may conduct criminal proceedings prescribed by this Law within the territory of the People's Republic of China without the approval of the competent authority of the People's Republic of China, and no institution, organisation or individual within the territory of the People's Republic of China may provide evidentiary materials and assistance prescribed by this Law to foreign countries.'

V COMPANY POLICIES AND PRACTICES

At this stage, Chinese law has no universal requirements for network operators to establish a complete privacy management programme. The CSL only provides some high-level generic network security requirements. For example, under the CSL network operators should formulate internal security management systems and operating instructions, determine the persons responsible for cybersecurity, and implement the responsibility for cybersecurity protection. In addition, network operators shall formulate contingency plans for cybersecurity incidents, and promptly deal with system bugs, computer viruses, network attacks and intrusions and other security risks; network operators shall adopt technical measures and other necessary measures to ensure the security of the personal information they have collected and prevent such information from being divulged, damaged or lost. If personal information has been or may be divulged, damaged or lost, it is necessary to take remedial measures immediately, inform users promptly according to the provisions and report the same to the relevant competent departments.

The Specification provides that a personal information controller is required to fulfil the requirements as below:

a it shall make clear that its legal representative or the chief in charge of the controller shall undertake the overall leadership responsibility for personal information, including guaranteeing the human resources, financial resources and materials needed for the work to ensure personal information security;

b it shall appoint a head in charge of personal information protection and set up an agency in charge of personal information protection;

c it shall establish a system for personal information security impact assessment, and assess the personal information security impact regularly (at least once a year);

d it shall develop its data security capability and put into place necessary managerial and technical measures in accordance with the rules specified in applicable national standards, to avoid personal information being leaked, destroyed or lost; and

e it shall audit the effectiveness of its privacy policies, relevant rules and processes, and security measures.

It is noteworthy that the Specification elaborates on the content of a privacy policy and also provides a privacy policy template for enterprises to refer to:

a basic information about this personal information controller, including its registered name, registered address, regular business office, contact of its head, etc.;

b purposes for which personal information will be collected and used, and what business functions are involved in these purposes, for example, using personal information in pushing commercials or creating direct user profiles and the use thereof;

c what personal information will be collected under each business function, the rules on the processing of personal information, including how and how often this information will be collected and where and how long this information will be stored, and the scope of personal information it actually collects;

d purposes for which personal information is shared with, transferred to, or publicly disclosed among, external parties, categories of personal information concerned, categories of third parties that receive the personal information, and the legal liability it bears;

e what basic principles it observes for the security of personal information, what capacity it has for data security, and what safeguards it has taken to ensure the security of personal information;

f the rights of personal information subjects and the mechanism to exercise these rights, such as how to access, modify and delete their own personal information, how to cancel the account, how to withdraw their consent, how to obtain a copy of their own personal information, and how to impose limits on the information system's automatic decision-making;

g likely security risks after personal information subjects have provided their personal information, and potential impacts that may arise if they refuse to provide such information; and

h in what ways and under what mechanisms enquiries and complaints filed by personal information subjects will be handled, and the department in charge of handling external disputes and its contact information.

VI DISCOVERY AND DISCLOSURE

Article 18 of the Anti-Terrorism Law requires that

> *telecommunications business operators and internet service providers shall provide technical interface, decryption and other technical support and assistance for the prevention and investigation of terrorist activities conducted by public security authorities and national security authorities in accordance with the law.*

In addition, the Specification stipulates that in principle personal information shall not be publicly disclosed. A personal information subject shall attach enough importance to risks and comply with the relevant requirements if it is truly necessary to publicly disclose the information upon legal authorisation or with justified reasons. And it shall assess the personal information security impact in advance and take effective measures to protect personal information subjects according to the assessment findings. It shall inform personal information subjects of the purposes for which their personal information will be publicly disclosed and what categories of information will be publicly disclosed and obtain the authority and consent of personal information subjects in advance. However, a personal information controller need not seek the authority and consent of personal information subjects in advance where:

a the sharing, transfer or public disclosure is in direct relation to state security or national defence security;

b the sharing, transfer or public disclosure is in direct relation to public security, public sanitation, or major public benefits;

c the sharing, transfer or public disclosure is in direct relation to investigations into crimes, prosecutions, court trials, execution of rulings, etc.;
d the sharing, transfer or public disclosure is for the sake of safeguarding significant legal rights and interests, such as the life and property, of personal information subjects or other individuals, but it is difficult to obtain their consent;
e the personal information to be shared, transferred or publicly disclosed is voluntarily made public by personal information subjects themselves; and
f the personal information is collected from information that has been legally and publicly disclosed, such as legal news reports and information published by the government.

Therefore, if for the purpose mentioned above, government agencies may require personal information controllers to publicly disclose personal information.

Information disclosure required by foreign government agencies shall comply with Article 4 of the Law on International Criminal Judicial Assistance.

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

Article 8 of the CSL provides that 'The national cyberspace administration authority is responsible for the overall planning and coordination of cybersecurity work and relevant supervision and administration work. The competent telecommunication department of the State Council, public security departments and other relevant authorities shall be responsible for protecting, supervising and administering cybersecurity within the scope of their respective responsibilities in accordance with the provisions of this Law and other relevant laws and administrative regulations. Responsibilities of relevant departments under local people's governments at or above the county level for protecting, supervising and administering cybersecurity shall be determined in accordance with the relevant.'

For undesirable practices, the main measure taken by the CAC is to interview the responsible persons of relevant network operators. For example, on 6 January 2018, the Network Security Coordination Bureau of the CAC interviewed relevant representatives of Alipay and Zhima Credit and pointed out that the way of using and collecting personal information in Alipay and Zhima Credit is not in line with the spirit of the Specification.

The competent telecommunications department under the State Council (i.e., the MIIT) from time to time issues notifications to organise and carry out administrative checks on network security in the telecommunications and Internet industries. For example, on 30 May 2019, the Network Security Administration of the MIIT issued a circular on the administrative inspection of network security in the telecommunications and internet industries in 2019, requiring all telecommunications and internet enterprises to cooperate in the network security inspection work.[11] At the same time, local telecommunications authorities usually notify enterprises that fail to implement their network security obligations.

11 MIIT, the Circular on Doing a Good Job in the Administrative Inspection of Network Security in the Telecommunications and Internet Industries in 2019. http://www.miit.gov.cn/n1146285/n1146352/n3054355/n3057724/n3057729/c6983820/content.html.

For example, on 12 July 2018, the Shanghai Communication Administration notified four internet enterprises that their network security requirements had not been implemented effectively.[12]

The MPS is mainly responsible for the protection of cybersecurity levels. For example, it issued the Regulation on Network Security Graded Protection (Draft for Comment) in June 2018 and the Provisions on Internet Security Supervision and Inspection by Public Security Organs in September 2018. At the same time, the MPS has launched the campaign 'Network Clearance Campaign' to punish illegal activities on the internet.[13]

In recent years, with the frequent occurrence of security incidents on mobile internet, the China Consumers Association began to study this and released the Assessment Report on Collection of Personal Information by and the Privacy Policy of 100 Apps.[14]

In addition, the competent authorities of various industries also have the right to supervise violations in their industries. For instance, the Notice of the People's Bank of China on Issuing the Implementation Measures of the People's Bank of China for Protecting Financial Consumers' Rights and Interests provides that 'A financial consumer shall, when having any dispute on financial consumption with a financial institution, file the complaint with the financial institution first in principle. If the financial institution refuses to accept the complaint or fails to handle the complaint within a certain time limit, or the financial consumer is of the opinion that the financial institution's handling result is irrational, the financial consumer may file a complaint with the PBC branch at the place where the financial institution is located, the disputes occur or the contract is signed.'

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

Foreign organisations face significant compliance challenges in relation to data localisation requirements. Article 37 of the CSL provides that:

> *Critical information infrastructure operators shall store personal information and important data gathered and produced during operations within the territory of the PRC. Where it is really necessary to provide such information and data to overseas parties due to business requirements, a security assessment shall be conducted in accordance with the measures formulated by the national cyberspace administration authority in concert with the relevant departments under the State Council. Where the laws and administration regulations have other provisions, those provisions shall prevail.*

However, since the promulgation of the CSL, there have been no clear definitions for the terms CII and 'important data'. It is difficult for foreign organisations to predict whether they will fall under the strict data localisation rules.

12 MIIT, The Shanghai communication administration notified four Internet companies that the implementation of network security requirements was inadequate. http://www.miit.gov.cn/n1146285/n1146352/n3054355/n3057724/n3057733/c6254778/content.html.

13 The MPS notification of launching the 2018 'Net Action' campaign, http://www.mps.gov.cn/n2254536/n2254544/n2254552/n6422073/index.html; The MPS notification of typical cases of launching the2019 'Net Action' campaign, http://www.mps.gov.cn/n2254536/n2254544/n2254552/n6528162/index.html.

14 China Consumers Association, Assessment Report on Collection of Personal Information by and Privacy Policy of 100 Apps.

Nevertheless, a number of industries have also enacted restrictions on specific data localisation, as descrived below.

i Banking

The Notice of the People's Bank of China on Urging Banking Financial Institutions to Do a Good Job in Protecting Personal Financial Information and the Notice of the People's Bank of China on Issuing the Implementation Measures of the People's Bank of China for Protecting Financial Consumers' Rights and Interests both provide that personal financial information acquired inside China shall be stored, processed and analysed inside China and no personal financial personal information acquired inside China should be transferred abroad, except as otherwise required by law, regulation or provisions.

ii Insurance

Article 82 of the Standards for the Financial and Accounting Work of Insurance Companies (2012) requires that 'the business and financial data in the financial information system of an insurance company shall be stored inside the territory of China and backed up offsite.'

iii Credit investigation industry

Article 24 of the Regulation on the Administration of Credit Investigation Industry provides that credit investigation institutions shall arrange, save and process information collected inside China within the territory; and if transferring the information abroad, it shall abide by relevant laws and regulations.

iv Mails and express mails

Article 16 of the Measures for the Administration of the Real-Name Receipt and Delivery of Mails and Express Mails provides that delivery enterprises should store the user information and important data collected and generated by it during its receiving and sending activities inside China within the territory.

v Population health information

Article 10 of the Measures for the Administration of Population Health Information provides that responsible units shall not store information on the population on any server outside China, nor shall they host or lease any server outside China.

Article 30 of the National Health and Medical Big Data Standards, Safety and Service Management Measures (trial) provides that specifies that, if it is indeed necessary to provide health and medical Big Data abroad due to business needs, it shall be subject to security assessment and audit as required by relevant laws and regulations.

vi Online taxi-booking business operations and services

Article 27 of the Interim Measures for the Administration of Online Taxi Booking Business Operations and Services provides that an online taxi booking platform company shall store and use the personal information collected and business data formed in China; and the information and data shall not be provided abroad, unless otherwise required by laws and regulations.

vii Map

Article 34 of the Regulation on Map Management provides that an internet map service entity should set the server storing map data inside China.

viii Network of civil aviation

Article 28 of the Interim Measures of Civil Aviation Network Information Security Management (Draft for Comment) stipulates that personal information and important data collected and generated by important information systems in operation inside China shall be stored within the territory.

IX CYBERSECURITY AND DATA BREACHES

The CSL is more focused on cybersecurity than personal information protection and has proposed the concepts of 'network operation security' and 'network information security'. Article 21 of Chapter III (Network Operation Security) provides that the state implements multi-level protection scheme for cybersecurity and network operators should prevent the network from interference, damage or unauthorised access and network data from being divulged, stolen or falsified.

Article 25 of the CSL provides that network operators should formulate contingency plans for cybersecurity incidents and deal with system bugs, computer viruses, network attacks and intrusions in a timely manner; if the incident endangers cybersecurity, network operators shall immediately initiate the contingency plan, take remedial measures and report to the relevant competent authority.

In addition, the CSL provides separately that operation security of CII. The CII is related to national economy and people's livelihoods, national security and public interests, and involves important industries and fields such as public communication and information services, energy, transportation, water conservancy, finance, public services and e-government. But the CSL does not specify the specific scope of CII and security protection methods.

According to the Article 21 of the CSL, all network operators in China are obligated to participate in the multiple -level protection scheme (MLPS). From late 2018 to May 2019, the MPS and other departments jointly issued several national standards on the MLPS. These standards include network infrastructure, important information systems, large internet websites, big data centres, and cloud computing platforms, 'internet of things' systems, industrial control systems, and public service platforms. In addition, these standards put forward new security expansion requirements for new technologies of cloud computing, internet of things, mobile internet, industrial control and big data.

Article 40 of Chapter IV Network Information Security provides that 'Network operators shall strictly keep confidential users' personal information that they have collected, and establish and improve the users' information protection system.' Article 55 of the CSL provides that 'For the occurrence of cybersecurity incidents, it is necessary to activate contingency plans for cybersecurity incidents immediately, investigate and assess such incidents, require network operators to take technical measures and other necessary measures to eliminate potential security hazards, prevent expansion of the harm, and promptly issue warning information in relation to the public to society.'

X OUTLOOK

With the promulgation of the CSL, the Chinese data protection and cybersecurity legal regime has taken shape rapidly. China is drafting a separate Data Security Law and a Personal Information Protection Law, and these are expected to be passed in the next four years. These new laws will also be part of China's legal regime of cybersecurity and data protection.

Chapter 9

COLOMBIA

Natalia Barrera Silva[1]

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.

1 Natalia Barrera Silva is a partner at Márquez, Barrera, Castañeda & Ramírez.

II THE YEAR IN REVIEW

During the past year there have been many developments in the data protection field in Colombia. In October 2018, Mr Nelson Remolina was appointed as the new Data Protection Delegate. Mr Remolina comes from the academic community and is known to have strong and conservative views on the protection of personal information.

Under his direction, SIC concluded many investigations on the infringement of data protection rules, imposing fines that exceeded the equivalent of US$550,000. Since the start of the new Data Protection Delegate's term, SIC has imposed fines on many large and renowned companies such as Claro (the largest mobile phone operator in the country), Directv, Avantel, Falabella Bank and Bancolombia Bank. These decisions were issued by the Directorate of Investigations on Personal Data Protection and were appealed by the interested parties before new Delegate.

SIC has also made other important decisions with international repercussions. In January 2019, SIC ordered Facebook Inc and its subsidiaries, Facebook Colombia SAS and Facebook Ireland Limited, to adopt new security measures and improve existing ones to guarantee the protection of the personal data of more than 31 million Colombian users of that network. Similarly, in July 2019, SIC ordered a multinational collaborative platform to develop and implement a comprehensive information security programme, which guarantees the security, confidentiality and integrity of the platform users. No fines were imposed in these cases.

On matters related to the National Registry of Databases, it is important to mention that on 31 January of 2019 the last deadline for controllers to register their databases in the Registry expired. This deadline had already been extended twice and in 2018, the government established a new threshold to limit registration to companies that have assets over approximately US$7 million. The next mandatory deadline to update the information included in the databases was 23 August 2019.

Finally, regarding data protection compliance within the government sector, the Attorney General's Office issued Resolution 462 of 2019, which assigned one of its departments the task of monitoring compliance by public authorities with data protection law.

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;[2]

c instructions and guidelines issued by SIC, the data protection authority; and

d Resolution 462 of 2019, regarding compliance with data protection regulation by public authorities.

2 Regulatory Decrees No. 1727 of 2009, 2952 of 2010, 1377 of 2013 and 886 of 2014.

ii Principles

Law 1581 sets forth the main principles applicable to the processing of data,[3] 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.

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.

iii 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.

3 Law 1581, Title II, Article 4.

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 eight 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, in relation 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,[4] 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[5] (specifically, the social security system and medical history), and related to employment relationships.[6]

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.

4 Article 7, Law 1581 of 2012.

5 See, for example, Resolution No. 1995 of 1999 of the Ministry of Health, Decisions C-264 of 1996 and T-1105/05.

6 See, for example, Decisions T-768/08 and T-405/2007 of the Constitutional Court.

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.

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[7] 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,[8] 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; or

7 Council CONPES No. 3920 of 'National Policy of Data Exploitation', National Department of Planning.
8 Article 26, Law 1581 of 2012.

f the transfer is 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.[9]

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.

9 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; Italy; Japan; Latvia; Lithuania; Luxembourg; Malta; Mexico; Norway; the Netherlands; Peru; Poland; Portugal; the United Kingdom; the Czech Republic; the Republic of Korea; Romania; Serbia; Sweden; and countries that are considered to have an adequate level of protection by the European Commission.

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.

Las 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:

a impose fines of up to 2,000 times the minimum wage;
b order the suspension of activities related to data processing for up to six months while corrections are implemented;
c order temporary closure of all operations related to processing when correctives are not implemented during the suspension; and
d 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

Order aimed at strengthening security measures

Based on the investigations and actions of data protection authorities of eight countries in the world (Ireland, the United States, the United Kingdom, France, the Netherlands, Canada, Australia and New Zealand) and legal proceedings initiated by the District Attorney General from Columbia (United States), SIC ordered Facebook Inc and its subsidiaries, Facebook Colombia SAS and Facebook Ireland Limited, to adopt new, necessary, appropriate, useful, demonstrable and effective measures to comply the principle and duty of security. Compliance must be certified by means of an independent audit, which must be carried out within the four months following the execution of Resolution 1321 of 2019 and every year after this date during the next five years. The guidelines were issued on a preventive basis to prevent other security incidents from happening, so no monetary penalty was imposed.

Fine for failing to delete contact data from databases

Colombia's first unicorn start-up company was recently fined for failing to suppress the contact data of a user after the user had asked the company to delete his data from all databases of the company. Once it received the request, the company delayed the response for four months and 25 days, when the maximum period established by law is 15 days. Finally, SIC took into account that during the administrative investigation, the company did not provide any evidence that the user had accepted the terms and conditions set forth in the mobile app, nor granted the corresponding authorisation for the processing of personal data. This decision has created uncertainty in the digital platforms, since many of them obtain authorisation through the same means as the company sanctioned did (acceptance of the privacy policy and terms and conditions when registering on the site).

Imposition of orders to demonstrate compliance with the principle of accountability

A multinational sharing economy company suffered a security incident in 2016 affecting the personal data of 57 million users (267,000 Colombian residents). According to the principle of accountability set forth in Colombian data protection regulation, data handlers must be able to demonstrate, at the request of SIC, that they have implemented appropriate and effective measures to comply with the obligations set forth in Law 1581 of 2012. In light of the above, SIC ordered the parent company and its subsidiaries to develop, implement and maintain a comprehensive information security programme, which guarantees the security, confidentiality and integrity of personal data, preventing adulteration, loss, consultation, use or unauthorised or fraudulent access. Furthermore, SIC considered that the company had taken too long to report the incident, and therefore ordered the company to develop, implement and maintain a programme for the management of personal data security incidents, that contemplates procedures to inform said authority and the data subjects. The guidelines were issued on a preventive basis to prevent other security incidents from happening, so no monetary penalty was imposed.

Private litigation

Law 1581 does not provide for specific remedies or financial recovery for private plaintiffs. Other actions such as class contractual or tort actions are also available to data subjects, though they are still not common.

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

According to Law 1581,[10] 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.

ii 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.

X 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.

10 Article 2, Law 1581 of 2012.

Chapter 10

CROATIA

Sanja Vukina[1]

I OVERVIEW

The Croatian Constitution, which entered into force on 22 December 1990, established privacy and protection of personal data as fundamental rights, stipulating legal protection of personal and family life, home, dignity, reputation and honour[2] and in addition guaranteeing the security and confidentiality of personal data.[3] Pursuant to the wording of the Constitution, personal data may be processed and used only with the data subject's consent or in accordance with the conditions prescribed by law. Additionally, the use of personal data contrary to the established purpose of their collection is prohibited.[4]

The Constitution established protection of personal data as a fundamental right. However, the implementation and further development of personal data protection legislation was lacking until 2003 when the Croatian parliament, under the influence of the Directive 95/46/EC[5] and the Council of Europe Treaty 108,[6] adopted the Personal Data Protection Act,[7] which established the Croatian Data Protection Agency (CPDPA), and until 2018 represented the general fundamental framework law regulating the field of data protection in Croatia.[8]

Since Croatia joined the EU on 1 July 2013, the EU *acquis communautaire* also became a part of the Croatian legal system. Particularly important is the Charter of Fundamental Rights of the European Union[9] (the Charter) which has foreseen the protection of personal data as a fundamental right, therefore stipulating that personal data may be processed only if 'processed fairly for specified purposes and on the basis of the consent of the person

1 Sanja Vukina is a partner at Vukina & Partners Ltd.

2 Constitution of the Republic of Croatia, Official Gazette 56/1990, 135/1997, 113/2000, 28/2001, 76/2010, 5/2014, Article 35.

3 ibid., Article 37.

4 ibid., Article 37.

5 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, OJ L 281, 23 November 1995, p. 31–50.

6 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 108.

7 Official Gazette 103/2003.

8 Croatian Data Protection Agency, Campaign for Raising Awareness Regarding Data Protection and privacy rights, accessed 4 July 2019 https://azop.hr/images/dokumenti/217/zastita_op_rh.pdf.

9 OJ C 326, 26 October 2012, p. 391–407.

concerned or some other legitimate basis laid down by law'.[10] Moreover, the Charter has also envisaged as fundamental rights the right to access and the right to rectify one's own personal data in addition to the obligation that an independent authority supervise compliance with the data protection rules. In May 2016, what is known as the EU data protection package,[11] that is, Regulation (EU) 2016/679[12] (GDPR) and Directive (EU) 2016/680[13] (DPLED), was adopted and alongside the Directive 2002/58/EC[14] (the ePrivacy Directive), which established a harmonised framework in the EU for the protection of online privacy, represents a fundamental data protection legal framework in the EU. At the time of writing, the ePrivacy Regulation[15] has still not been adopted.

In order to comply with the GDPR and DPLED, the Croatian parliament adopted the General Data Protection Regulation Implementation Act[16] (the Implementation Act), which entered into force on the same day as the GDPR, and the Act on the protection of natural persons with regard to the processing and exchange of personal data for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties (the DPLED Implementation Act)[17] entering into force shortly afterwards. The provisions of the ePrivacy Directive were transposed in the Croatian legal system through the Croatian Electronic Communications Act (ECA).[18]

Despite the general framework regarding the protection of personal data established by GDPR together with the Implementation Act, sector-specific acts (e.g., the Labour Act, ECA, Act on Data and Information in Health Care, Insurance Act, etc.) still provide data protection particularities generally regarding the means of processing or processing purpose.

10 Charter of Fundamental Rights of the European Union, OJ C 326, 26 October 2012, p. 391–407, Article 8 (2).

11 https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en, accessed 4 July 2019.

12 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L 119, 4 May 2016, p. 1–88.

13 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.

14 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31 July 2002, p. 37–47, amended by: Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006, OJ L 105, 13 April 2006, p. 54, Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, OJ L 337, 18 December 2009, p. 11, corrected by Corrigendum, OJ L 241, 10 September 2013, p. 9.

15 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) COM/2017/010 final – 2017/03 (COD), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017PC0010, accessed on 11 July 2019.

16 Official Gazette 42/2018.

17 Official Gazette 68/2018.

18 Official Gazette 73/2008, 90/2011, 133/2012, 80/2013, 71/2014, 72/2017.

To the best of our knowledge, no Croatian NGOs or self-regulatory industry groups have taken any significant actions regarding privacy and protection of personal data.

Regarding Croatia's approach to cybersecurity, on 7 October 2015, the Croatian government adopted the National Cybersecurity Strategy with the accompanying action plan for carrying it out. Its 'ultimate goal . . . [is] to facilitate efficient execution of the laws and regulations and the protection of democratic values in the virtual dimension of contemporary society, i.e. cybernetic space'.[19] Furthermore, the Act on Cybernetic Security of Key Services Providers and Digital Service Providers (the Cybernetic Security Act')[20] implementing Directive (EU) 2016/1148[21] entered into force on 26 July 2018, and along with the Ordinance on Cybernetic Security of Key Services Providers and Digital Service Providers (the Cybernetic Security Ordinance), which entered into force on 4 August 2018, further regulates the measures and procedure regarding the safety of key service providers and digital service providers, establishing the general framework of cybersecurity regulation in Croatia.

II THE YEAR IN REVIEW

Even though GDPR has already been in force for over a year, owing to frequent and somewhat fatalistic coverage from the media, the GDPR became a source of worry for health and education service providers and business entities particularly dealing with consumers, such as financial services providers, insurance providers, marketing services providers, hospitality service providers and online retailers. Although the GDPR was highly covered by the media, there are still a vast number of entities that have not fully complied with the GDPR. Furthermore, some entities have decided to refrain from particular actions and others have temporarily ceased some of their actions until they sufficiently comply with the GDPR. This is the case for the Croatian Register of Credit Liabilities, which has temporarily stopped providing credit reports regarding consumers, tradesmen and family farmers until they arrange a way of collecting and processing personal data in compliance with the GDPR.

Moreover, the GDPR still raises a lot of problems since the rules for certain processing activities are not completely clear and the potential fines are high. To tackle the issue, the CPDPA almost doubled in size and issued a number of public opinions on frequently asked questions. Since the GDPR's entry into force, the CPDPA has already, inter alia, issued opinions regarding personal data processing of employees, credit debtors and children, the processing of personal data in educational and health institutions, the processing of personal data in marketing and processing of personal data via means of video surveillance. Particularly interesting are the opinions of 5 June 2019 regarding the Processing of Personal Data for the Collection of Overdue and Unpaid Claims by Companies/Agencies for Collecting Receivables and that of 7 June 2019 regarding Video Surveillance-Streaming.

In the opinion of 5 June 2019, the CPDPA stated that since the contract of assignment is regulated by the Civil Obligations Act, the processing (transfer and debt collection) of

19 Summary of the National Cybersecurity Strategy, accessed on 4 July 2019 https://www.uvns.hr/hr/normativni-akti/informacijska-sigurnost/kiberneticka-sigurnost.

20 Official Gazette 64/2018.

21 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19 July 2016, p. 1–30.

debtors' personal data required for collecting the claim should be considered carried out on the legal basis of the particular law (i.e., the Civil Obligations Act) since the transfer of the claim presupposes the delivery of personal data. Furthermore, the aforementioned opinion stated that the contract's terms and conditions frequently inform the debtors of the possibility for creditors to assign their claim against the debtor to companies and agencies for collecting receivables and by such notification creditors (assignor and assignee) fulfil their obligations to inform debtors under Article 13 or 14 of the GDPR in relation to such transfer.[22]

In the opinion issued on 7 June 2019, the CPDPA stated that livestreaming of public spaces by means of webcams, where the films are not stored or there is no possibility to retroactively access the films, are not subject to the GDPR, since the latter only applies to the processing of personal data wholly or partly by automated means that form a part of a filing system or are intended to form part of a filing system.[23]

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

The GDPR defined all the relevant main terms and the Implementation Act has unambiguously by a general provision[24] accepted those terms defined in GDPR as its own. Therefore, there are no deviations regarding their meaning from the meanings ascribed to them by GDPR.

Pursuant to GDPR, two types of personal data exist, personal data and special categories of personal data ('sensitive data').

Personal data is defined as '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'.[25]

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'[26] are considered as sensitive data and generally the processing of such data is prohibited, except when done pursuant to the exceptions prescribed in the GDPR and under certain conditions if they are prescribed by national legislation. As prescribed by the GDPR, national legislation may particularly 'introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health'.[27] The Implementation Act has introduced further conditions regarding the processing of the foregoing.

Under the GDPR and the Implementation Act the entity (natural or legal person) that determines the purpose and means of processing of personal data is considered

22 https://azop.hr/misljenja-agencije/detaljnije/obrada-osobnih-podataka-u-svrhu-naplate-dospjelih-a-nenaplacenih-trazbina-o, accessed on 5 July 2019.

23 https://azop.hr/misljenja-agencije/detaljnije/videonazdor-livestreaming, accessed on 5 July 2019.

24 'Terms for the purposes of this Act shall have the same meaning as the terms used in the General Data Protection Regulation.', Implementation Act, Article 3.

25 GDPR, Article 4 (1) item 1.

26 ibid., Article 9.

27 ibid.

a 'controller',[28] while the entity that processes on behalf of the controller is considered a 'processor'.[29] Processing 'means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction'.[30]

The Implementation Act prescribed that the CPDPA shall act as a supervisory authority under the GDPR and DPLED and also as an accreditation body under the Regulation (EC) No. 765/2008,[31] the internal requirements and scope of work of the CPDPA, the CPDPA's rules of procedure and legal remedies against the CPDPA's decision, additional requirements for the processing of personal data regarding children, genetic data, biometric data, processing data by video surveillance and processing data for statistical purposes.

Regarding the protection of consumers, the Implementation Act did not prescribe any additional requirements; however, the Croatian Consumer Protection Act contains a provision stating that 'the retailer shall be prohibited from providing personal data to any third party without the prior consent of the consumer, in accordance with the law governing the protection of personal data'.[32] In regard to the aforementioned and since the GDPR expressly stipulates that 'the free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data',[33] the applicability and the extent of the aforementioned provision of the Consumer Protection Act is currently not clear. However, it may be observed that business entities have largely relied solely on the provisions of the GDPR rather than on the aforementioned provision of the Consumer Protection Act.

ii General obligations for data handlers

Both controllers and processors who process personal data of data subjects who are in the EU, regardless of where the processing occurs and therefore including entities established outside the EU that process personal data as controllers or processors, offer goods in the EU or monitor the behaviour of data subjects in the EU as far as their behaviour takes place within the EU, must comply with the provisions of the GDPR.[34]

Furthermore, GDPR 'applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system', save when processing occurs in the course of purely personal or household activity, in the course of an activity that falls outside the scope of EU law, when Member States of the EU carry out activities that fall within the scope of Chapter 2 of Title V of the TEU,[35] by competent

28 ibid., Article 4 (1) item 7.

29 ibid., Article 4 (1) item 8.

30 ibid., Article 4 (1) item 2.

31 Regulation (EC) No. 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No. 339/93 (Text with EEA relevance), OJ L 218, 13 August 2008, p. 30–47

32 Consumer Protection Act, Official Gazette 41/2014, 110/2015, 14/2019, Article 11.

33 GDPR, Article 1 (3).

34 ibid., Article 3.

35 Treaty on European Union, OJ C 326, 26 October 2012, p. 13–390, consolidated version.

authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.[36]

Namely, in order to comply with the GDPR, personal data should be processed in accordance with the principles laid down under the GDPR, therefore entities processing personal data must:

a have a legal basis for processing as prescribed under the GDPR ('principle of lawfulness'), and so must provide one of the following legal bases:
- have the data subject's consent;
- be necessary for the performance of a contract to which the data subject is a party of or in order to take steps at the request of the data subject prior to entering into a contract;
- comply with controllers' legal obligation under law;
- be necessary for protection of data subject's or another natural persons vital interest;
- be necessary for the performance of tasks carried out in the public interest or in the exercise of official authority vested in the controller; or
- be a legitimate interest pursued by the controller or third party;[37]

b have a specified, explicit and legitimate purposes for processing (e.g., for marketing, provision of services) ('purpose limitation principle');

c collect accurate and when necessary up to date personal data ('accuracy principle');

d refrain from collecting excessive personal data that is not relevant for the purpose of processing ('data minimisation principle');

e process the personal data in a secure way, particularly protect the personal data from unauthorised access and destruction or loss of personal data ('integrity and confidentiality principle');

f keep the personal data in a form that permits identification of data subjects for no longer than is necessary for the purposes ('storage limitation principle'); and

g inform the data subject of all the relevant information (as applicable in Articles 13 and 14 of the GDPR) regarding the processing of the data subject's personal data in a way that would not deceive or mislead data subjects regarding the processing of their personal data (the 'transparency principle' and 'fairness principle').

When an entity acts as a controller, he must be able to demonstrate compliance with all the aforementioned principles applicable when processing data subject's personal data (the 'accountability principle').[38]

Particularly important for complying with the GDPR is the controller's obligation to notify the data subject regarding the processing of his or her personal data. Notifications to the data subject should contain information understandable to the data subject, inter alia, regarding the identity of the controller, contact details of the data protection officer, purposes of processing and intended legal basis of processing, categories of personal data,

36 GDPR, Article 2.

37 ibid., Article 5 and 6.

38 ibid., Article 5.

recipients of personal data, intention regarding the transfer of personal data to recipients in third countries, existence and enforcement of the data subject's rights and others as prescribed under Articles 13 or 14 of the GDPR.

Furthermore, under the GDPR, a record of processing activities must be established by controllers employing 250 or more persons or when processing is not occasional and shall likely result in a risk to rights or freedoms of the data subject or when sensitive data are being processed.

Controllers and processors that process personal data carried out by a public authority or body, except for courts acting in their judicial capacity shall have the obligation to designate a data protection officer (DPO) when their core activities consist of:

a processing operations that by virtue of their nature, scope or purpose, require regular and systematic monitoring of data subjects on a large scale; or

b processing sensitive data and personal data relating to criminal convictions and offences on a large scale.[39]

Even though the DPO may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract, the DPO should also have professional qualities and, in particular, expert knowledge of data protection law.[40] DPOs directly report to the highest management level of the controller or the processor; however, in performing their task they do not receive any instructions regarding the exercise of their tasks from the controller or processor.[41] DPOs, inter alia, inform and advise the controller or the processor regarding their obligations under the law, monitor compliance with respective data protection provisions and internal data protection policies, providing advice where requested on the data protection impact assessment and communicate with the supervisory authority.[42]

Pursuant to the previous Croatian Data Protection Act, controllers had the obligation to establish a personal data database and deliver to the CPDPA records regarding personal data databases;[43] however this obligation has been removed under the GDPR and Implementation Act.

iii Data subject rights

Data subjects under Articles 15–22 of the GDPR, with alterations depending on the basis of processing, have the following rights:[44]

a the right of access: the data subject's right to obtain from the controller a confirmation if the personal data relating to the data subject is processed by the controller) and if the controller processes data subject's personal data, to gain access to data subject's personal data and information regarding, inter alia, processed personal data, the purpose of processing, storage period, categories of recipient and particularly deliveries to third countries, etc.;

39 ibid., Article 37.

40 ibid.

41 ibid., Article 38.

42 ibid., Article 39.

43 Croatian Data Protection Act, Article 16.

44 https://azop.hr/prava-ispitanika/detaljnije/osnovna-prava-ispitanika, CPDPA general rights of data subjects, accessed on 11 July 2019.

b the right to rectification: the data subject's right to rectify his inaccurate personal data with the controller and supplementing additional personal data to the controller, including by providing a supplementary statement;

c the right to erasure ('right to be forgotten'): the data subject's right to obtain without undue delay the erasure of his or her personal data from the controller such as (i) when the processing of personal data is no longer necessary to the controller, (ii) data subject withdrew its consent and the processor has no other legal ground for processing, (iii) personal data have been unlawfully processed. However, the subject's right to erasure shall not apply to the extent that processing is necessary for, inter alia, exercising the right of freedom of expression and information and for the establishment, exercise or defence of legal claims;

d the right to restriction of processing: the data subject's right to obtain from the controller restriction of processing in certain situations such as (1) when the accuracy of the data is contested or (2) when 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 of defence of legal claims. However, where the processing has been restricted, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the EU or of a Member State;

e the right to data portability: the data subject's right to receive his or her personal data, which he or she has previously provided to the controller, in a structured form, commonly used and machine-readable format, and to transmit those data to another controller without hindrance by the controller to which the personal data are provided, where the processing is, pursuant to the GDPR, based on consent or contract and carried out by automated means;

f the right to object: the data subject's right to file an objection to the controller regarding the processing of personal data (including profiling) necessary for the performance of a task carried out in the public interest or in the execution of the official authority vested in the controller or on the legitimate interests of the controller. After objection to the aforementioned processing the controller shall no longer process the data subject's personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims. The GDPR prescribes that if the data subject's personal data were processed on the basis of a legitimate interest for direct marketing purposes, data subjects may object to such processing and the controller may no longer process such personal data; and

g the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal or similarly significant effects for the data subject, unless such a decision is (1) necessary to enter or perform a contract between the data subject and the controller, (2) authorised by EU law or by member state law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests or (3) based on the data subject's explicit consent.

iv Specific regulatory areas

Electronic marketing

Pursuant to ECA, the use of automatic calling or communication system without human intermediation, telefax devices or emails, including SMS and MMS messages, is allowed for the purpose of direct marketing and sale only with prior consent of subscribers or users, save as when the subscriber or the user is a legal entity. However, business entities, including both natural and legal entities, in the event that the consumer has not previously rejected such use of personal data, may use email addresses collected from its consumers when selling products and services only for direct marketing and sale of similar products and services, provided that such consumers have a clear and unambiguous possibility of free and simple objection to such use of email address in time of collection of their email address and each subsequent receipt of such email.[45]

On 19 April 2019, CPDPA issued its opinion[46] regarding the processing of personal data for the purpose of marketing in which it stated that under ECA relevant business entities may process personal data on basis of consent and legitimate interest in accordance with the foregoing rules provided in ECA. Furthermore, CPDPA particularly pointed out that it is not allowed to subsequently use the basis of legitimate interest in processing if there were problems with the validity of consent.

Regarding the validity of the consent, CPDPA expressly stated that consent must be a 'voluntarily, in particular, informed and unambiguous expression of the wishes of the data subject regarding the processing of his/her personal data, such as by declaration or clear confirmation, which could include marking the checkmark field when visiting web pages, selecting technical information service provider's settings or other statements or behaviours that clearly indicate in that context that the data subject accepts the proposed processing of his/her personal data. Silence, a pre-ticked checkmark, or lack of activity, should therefore not be considered as consent.'

Moreover, in the foregoing opinion CPDPA stated that official business email and official business mobile phones numbers are considered as official business data, however if it is possible to directly or indirectly identify a particular natural person using the structure of the official email (web protocol address), it shall also be considered as not only official business data, and in that case the provisions of the GDPR shall apply. However, it is important to point out that according to the respective opinion, CPDPA is of the stance that an official business email and official business mobile phone number may be used exclusively for the purpose of official (business) contact with a legal entity and may not be used for other purposes.

Children

Pursuant to the Implementation Act, a child's consent in relation to the direct offer of information society services shall be valid if a child is at least 16 years old and if the child's residence is in the Republic of Croatia.[47]

45 ECA, Article 107.

46 https://azop.hr/misljenja-agencije/detaljnije/obrada-osobnih-podataka-u-svrhe-marketinga, CPDPA Opinion dated 19 April 2019, accessed on 11 July 2019.

47 Implementation Act, Article 19.

Employment law

Regarding the processing of personal data in the context of employment the Croatian Labour Act (CLA)[48] prescribes that employee's personal data may be collected, processed, used and delivered to third parties only if this is provided by CLA or other law or, if necessary, for the purpose of exercising the rights and obligations arising from the employment relationship.[49] The foregoing shall be prescribed in advance in the employment rulebook, containing information regarding which personal data shall be collected, purposes of processing and third parties which may receive employees' personal data. Also, personal data may be delivered to third parties only by the employer or a person specifically authorised by the employer. Incorrect personal data must be corrected immediately and personal data for which legal or factual reasons do no longer exist must be deleted or otherwise removed.[50]

In addition, employer employing at least 20 employees is obliged to appoint a trustee who enjoys the trust of the employees (employee trustee) and who, except for the employer, is authorised to supervise if the collection, processing, usage and delivery of personal data to third parties are in accordance with the law.[51] To appoint the employee trustee, prior approval from the works council is necessary.[52] Namely, it is important to note that the employee trustee and the DPO is not always the same person since the employee trustee must be a person who enjoys the trust of employees and was approved by the work's council prior to his appointment.

The employer, the employee trustee and any other person who, in the performance of his or her duties, shall have access to the personal data of employees, must keep such data permanently confidential.[53]

Moreover, pursuant to the CLA, prior to making a decision important for the position of the employees, the employer must consult with the works council on the intended decision, and must provide the works council with information relevant to the decision making and the perception of its impact on the position of the employees. In case the employer does not comply with the foregoing obligation to consult with the works council the decision shall be pursuant to the CLA null and void.[54] Such consultations may be necessary in case the processing of employees' personal data is done in an intrusive way, such as when systematically monitoring employee emails, online logs of websites visited or 24-hour tracking of the movement of an employee's official vehicle or when using biometric employee data.[55] In relation to the aforementioned, the Implementation Act explicitly permits that controllers (employers) having establishment or offering services in Croatia may process employees' biometric data for the purpose of recording of working hours and for entering and leaving the official premises, provided that the employee has explicitly consented to such processing of biometric data in accordance with the provisions of the GDPR. However, it is not entirely clear if employers should always consult with the works council prior to processing employees' biometric data.

48 Official Gazette 93/2014, 127/2017.

49 CLA., Article 29.

50 ibid.

51 ibid.

52 ibid., Article 151 (1) item 8.

53 ibid., Article 29.

54 ibid., Article 150 (12).

55 ibid., Article 150.

Additionally, the Implementation Act prescribed that employees' personal data may be processed by means of video surveillance, except in premises intended as spaces of rest, personal hygiene and dressing rooms, only if the employees have been adequately informed, and if all the provisions laid down by regulations governing occupational safety and health care and the Implementation Act have been fulfilled.[56]

Video surveillance

Processing of personal data by means of video surveillance pursuant to the Implementation Act is allowed only for the purpose necessary and justified for protecting natural persons and property.[57] Controllers may conduct video surveillance regarding the foregoing purpose on the premises, parts of the premises, the outer surface of the object as well as the internal space in public transport.[58] When using video surveillance, the object must be designated with an easily intelligible picture containing text about the controller, contact details and information that the object is under video surveillance, visible at latest when entering the recording perimeter. Additionally, a notice containing all the relevant information under Article 13 of the GDPR must also be accessible to the data subjects (usually by stating the respective web address below the easily intelligible picture).[59] Records acquired by means of video surveillance may be stored for no longer than six months, save as prescribed otherwise by law, or if those records are evidence in a court or other equivalent proceeding.[60]

Furthermore, the Implementation Act additionally prescribes that to conduct video surveillance in residential or business and residential buildings, the approval of the owners owning at least two-thirds of the building is required.[61]

Health privacy

On 15 February 2019 the Act on Data and Information in Health Care (ADH)[62] entered into force, regulating the processing of health data and health information. Pursuant to ADH, health data is considered as data regarding the physical or mental health of an individual, including the data on provided health services in the Croatian health system, and health information is considered information generated by processing of health data for the purpose of its further use in the health system or for the needs of the system connected with the health system.[63] Both health data and health information may be considered sensitive data, or at least as personal data under the GDPR. Furthermore, ADH prescribes additional provisions, inter alia, regarding the quality, accessibility, data minimisation and transfer of health data and health information, also including the processing of personal data through the Central Health Care Information System and National Public Health Care Information System. Following from the foregoing, it would be advisable that entities providing health services,

56 Implementation Act, Article 30.
57 Implementation Act, Article 26.
58 ibid., Article 26.
59 ibid., Article 27.
60 ibid., Article 29.
61 ibid., Article 31.
62 Official Gazette 14/2019.
63 ADH, Article 3.

when informing their clients regarding the processing of health data and health information, also reflect in their privacy notices the applicable provisions of ADH regarding the processing of the data subject's personal data.

Insurance

The amendments to the Insurance Act,[64] which entered into force on 22 December 2018, explicitly prescribe that insurance companies are allowed to process health personal data when it is necessary to process health personal data to conclude and execute an insurance contract and enforcement of legal rights of the insured. From the wording of the relevant provision it may be concluded that the processing of health personal data regarding insurance contracts may be done on the legal basis of contract, however it should be noted that under GDPR the processing of sensitive data is generally prohibited, save as prescribed by Article 9(2) of the GDPR. The Final Proposal of the Act Amending the Insurance Act set forth a rationale stating that insurance activities may be considered as activities of public interest since they aim to preserve life conditions in the event of insured risk occurrence.[65] Furthermore, the Insurance act prescribed that, inter alia, insurance companies may process the national identification number and collect a copy of the identification document or bank card for the purpose of concluding and executing an insurance contract, and store personal data until the expiry of the respective statute of limitations period.[66]

Additionally, the Implementation Act prohibited, including on basis of data subject's consent, the processing of genetic data for calculating the chances of illnesses or other health conditions of data subjects when concluding or executing life insurance contracts or contracts including survivorship clause.[67] The foregoing applies when data subjects conclude the respective contracts in Croatia with controllers having establishment or offering services in Croatia.[68]

Company law

The Amendments to the Company Act implemented the EU Directive (EU) 2017/1132,[69] and added provisions regarding the processing of personal data of joint stock companies' stockholders, which shall enter into force on 1 January 2021. The relevant provision prescribed that the company and the intermediaries are entitled to process stockholders' personal data for the purposes of identifying, communicating, exercising stockholders' rights and cooperating with shareholders.[70] However, since the foregoing provision shall enter into force on 1 January 2021, joint stock companies and intermediaries until that time shall have to collect personal data on another legal basis pursuant to the GDPR. In addition, the Amendments to the Company Act have not foreseen a similar provision regarding the

64 Official Gazette 30/2015, 112/2018.

65 Final proposal of the Act Amending the Insurance Act, http://edoc.sabor.hr/Views/AktView.aspx?type=HTML&id=2023117, accessed on 12 July 2019, p. 125.

66 Insurance Act, Article 388.

67 Implementation Act, Article 20.

68 ibid.

69 Directive (EU) 2017/1132 of the European Parliament and of the Council of 14 June 2017 relating to certain aspects of company law (Text with EEA relevance.), OJ L 169, 30 June 2017, p. 46–127.

70 Company Act, Official Gazette 111/1993, 34/1999, 121/1999, 52/2000, 118/2003, 107/2007, 146/2008, 137/2009, 111/2012, 125/2011, 68/2013, 110/2015, 40/2019, Article 297.e.

processing of personal data of shareholders of other types of companies; therefore, companies must find an appropriate legal basis for processing the personal data of their shareholders and appropriately inform their shareholders.

v Technological innovation

Biometric data

Processing of biometric data, pursuant to the Implementation Act, is subjected to different provisions depending if the processing is done by bodies of public authority or entities carrying out business activities in the private sector. Public authority bodies may process biometric data only if it is prescribed by law and if it is necessary for protection of people, property, classified data and business secrets; however, entities acting in the private sector may process biometric data if it is prescribed by law or if it is necessary for protection of people, property, classified data, business secrets or safe identification of a user.[71] Therefore, entities acting in the private sector are free to choose any of the prescribed legal bases under the GDPR for such processing, save as for safe identification of a user in which case explicit consent must be obtained.[72]

Use of cookies

The ECA implemented Directive 2009/136/EC,[73] which amended the ePrivacy Directive in relation to the use of cookies. The ECA prescribed that the usage of electronic communication network for storing or accessing stored data in the terminal equipment of the subscriber or user is generally allowed only with prior consent after receiving a clear and complete notification pursuant to data protection regulations, particularly including the purpose of such processing.[74] However, such processing without explicit consent is allowed in cases (1) when storing technical data or accessing data in terminal equipment is required for the sole purpose of carrying out the transmission of a communication over an electronic communications network or (2) in order for the provider of an information society service to provide the service explicitly requested by the subscriber or user.[75]

IV INTERNATIONAL DATA TRANSFER AND DATA LOCALISATION

The provisions regulating the transfer of data are prescribed by the GDPR, the Implementation Act does not prescribe additional requirements for transferring personal data.

Pursuant to the GDPR, transfers within the EU are not treated differently than transfers within a Member State, while data transfers to non-EEA countries are allowed if in accordance with the GDPR.[76]

In that sense, under the GDPR, data transfers outside the EU may be executed on the basis of an adequacy decision (i.e., a prior European Commission decision deciding that a third country (e.g., Switzerland, Argentina)), a territory within the Member State, or the

71 Implementation Act, Article 21 and 22.

72 ibid.

73 Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, OJ L 337, 18 December 2009, p. 11–36, the 'Cookie Directive'.

74 ECA, Article 100 (4).

75 ibid.

76 GDPR, Article 1 (3) and Article 44.

international organisation ensures an adequate level of protection regarding protection of personal data; subject to appropriate safeguards (i.e., transfers based on, (1) a legally binding and enforceable instrument between public authorities or bodies, (2) transfers based on binding corporate rules, (3) standard data protection clauses adopted by the Commission or (4) by the data protection authorities, (5) approved codes of conduct or (6) approved certification mechanisms; and on specific situations derogations, such as when the data subject has explicitly consented to the proposed transfer, or if the transfer is necessary for the establishment, exercise or defence of legal claims.[77]

Pursuant to the GDPR, onward transfers (i.e., subsequent transfers done outside the EU) are also subject to the foregoing provision and requirements prescribed under the GDPR.[78]

V COMPANY POLICIES AND PRACTICES

Since the GDPR prescribes the obligation for controllers to notify data subjects regarding the processing of personal data, companies generally have an online or written privacy policy in their business premises for clients and consumers that contains information prescribed under Article 13 of the GDPR.

Medium and large companies that are more data-protection-oriented also tend to have internal privacy policies regarding the processing of employees' personal data and employees' rights and responsibilities regarding the processing of personal data of clients and consumers. Internal privacy policies may be included in the employment rulebooks or as a separate rulebook.

In addition to the foregoing, multinational companies mainly tend to have an internal corporate privacy policy regarding the sharing of personal data between affiliated companies and if applicable they also undergo a privacy impact assessment. On 21 December 2018, the CDPCA adopted the decision on establishing and publicly announcing the list of types of processing proceedings for which a privacy impact assessment must be undertaken,[79] in which it prescribed that a privacy impact assessment, inter alia, must be undertaken for:

a processing of personal data for systematic and extensive profiling or automated decision making for making conclusions which substantially effect or may affect the data subject's right of access to a service or benefit;

b processing of special categories of personal data for profiling or automated decision making;

c processing biometric or genetic data when at least one additional criteria from the Guidelines on Data Protection Impact Assessment (DPIA) (WP 248 rev 01) are fulfilled; and

d processing of employee personal data by applications or tracking systems.

77 ibid., Article 44–49.

78 ibid., Article 44.

79 https://azop.hr/aktualno/detaljnije/odluka-o-uspostavi-i-javnoj-objavi-popisa-vrsta-postupaka-obrade-koje-podli, accessed on 12 July 2019.

V DISCOVERY AND DISCLOSURE

Disclosure of personal data to Croatian public authorities is done generally on the basis of the law, while foreign authority requests may be executed if they comply with legally binding and enforceable instruments between the domestic and foreign public authority or on basis of necessity for reason of establishing, exercising or defending a legal claim.[80]

The Implementation Act explicitly excluded the application of the provision regarding biometrical data when processing personal data for reasons of defence, national security or security intelligence systems. Furthermore, when processing personal data in relation to national security and serious crime surveillance, the DPLED Implementation Act explicitly excluded its applicability when the processing and exchange of personal data is done during activities performed by the security intelligence bodies in the area of national security, activities related to matters of national security carried out by the defence system, as well as when processing and exchanging personal data in carrying out activities covered by Chapter V of Chapter 2 of the Treaty on the European Union.[81]

VI PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

The CPDPA is, pursuant to the Implementation Act, presented as an autonomous and independent national data protection authority as prescribed by the GDPR. The CPDPA is, inter alia, authorised to (1) when prescribed by law, initiate criminal, misdemeanour, administrative, and other court proceedings, be they court or out-of-court proceedings as a result of violations of the GDPR, (2) publicly announce particular decision, (3) initiate and conduct relevant proceedings against persons liable as a result of violations of the GDPR, (4) supervise the application of the DPLED, (5) issue opinions regarding the processing of personal data on the request of natural or legal entities and (6) order administrative monetary fines under the GDPR. Notwithstanding the foregoing under the GDPR, the CPDPA also acts as an advisory body regarding the processing of personal data.

Any persons who consider that their rights guaranteed under the GDPR and the Implementation Act are violated may submit a request to establish a violation of data subject's rights before the CPDPA. The CPDPA has the power to carry unannounced and announced investigations regarding their tasks and competences, pursuant to the CPDPA's director's order.[82] Moreover, if deemed necessary, the CPDPA is entitled to copy, seal and temporarily seize the storage systems or equipment.[83] When a breach of the GDPR or the Implementation Act is established, the CPDPA may issue warnings, reprimands, order the controller or processor to comply with the data subject's requests, impose a temporary or definitive limitation including a ban on processing, order a fine of up to €20 million and

80 Guidelines on Article 49 of Regulation 2016/679, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614232, accessed on 11 July 2019.

81 DPLED Implementation Act, Article 3 (2).

82 Implementation Act, Article 36.

83 ibid., Article 37.

order an erasure regarding the processed personal data. An administrative lawsuit may be initiated before the administrative court against the decisions, orders and other acts of the CPDPA.[84]

In the past and current year, the CPDPA has focused more on their advisory roles, therefore providing support regarding the compliance of entities with the provisions of the GDPR, rather than initiating enforcement proceedings against controllers. According to the proposed CPDPA annual work report for the year 2018, submitted to the Croatian parliament, the amount of the CPDPA's workload quadrupled. It received 4,901 enquiries, and 79 per cent of these consisted of requests to give legal opinions and answer questions regarding the implementation of the GDPR.[85]

ii Recent enforcement cases

The CPDPA has dealt with requests to establish violations of data subjects' rights due to public announcements of data subjects' personal data in the newspaper or other media and as a result of video surveillance on an object without complying with the necessary requirements under the Implementation Act or the GDPR. In most of the foregoing cases, the CPDPA did not establish that a violation of the data protection regulation had occurred and subsequently the data subjects submitted an administrative lawsuit against those decisions. In two cases, the CPDPA established a violation of data subjects' rights and ordered that the controller must erase the processed personal data and stop with the unlawful processing of personal data; however, it did not impose any monetary fines against the controllers.[86]

iii Private litigation

Private litigations regarding violations of a data subjects' right to privacy and data protection are quite rare and there has not been a developed case law thereof. Pursuant to GDPR it is possible to file a claim for damages if a controller violates the data subject's right prescribed under GDPR, however CPDPA or the courts have not issued any guidelines regarding the amount that may be claimed for violations of data subjects' rights. Furthermore, pursuant to the Croatian Civil Procedure Act,[87] particular entities may file a lawsuit for the protection of collective interests and rights – a type of lawsuit similar to a class action – but there has been no significant public interest regarding such a lawsuit.

VII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

Foreign entities should generally take higher precautions when processing employee-related personal data, sensitive data or processing personal data by means of video surveillance, since such processing may trigger the jurisdiction of the CPDPA as a result of potential complaints regarding such processing from the data subjects. Besides the foregoing, foreign organisations

84 ibid., Article 34.

85 Annual report of the CPDPA, https://www.sabor.hr/sites/default/files/uploads/sabor/2019-04-02/154602/IZVJESCE_AZOP_2018.pdf, accessed on 13 July 2019.

86 https://azop.hr/rjesenja-agencije/detaljnije/objava-osobnih-podataka-u-elektronickoj-medijskoj-publikaciji-udruge, accessed on 13 July 2019.

87 Official Gazette 53/1991, 91/1992, 112/1999, 129/2000, 88/2001, 117/2003, 88/2005, 2/2007, 96/2008, 84/2008, 123/2008, 57/2011, 25/2013, 89/2014.

that have affiliates in Croatia or offering services in Croatia must also have in mind that transferring employee or customer personal data outside the EU may potentially also trigger the jurisdiction of the CPDPA.

Generally, there are no localisation requirements regarding data servers or storage of personal data in relation to foreign organisations.

VIII CYBERSECURITY AND DATA BREACHES

Key service operators, pursuant to the Cybernetic Security Act, are obliged to undertake technical and organisational measures to (1) establish risks regarding incidents, (2) prevent, detect and solve incidents, and (3) mitigate the impact of incidents.[88] In the event of an incident, key service operators are obliged to report it to the competent computer security incident response team, which may with prior consultation with the key service operator announce to the public that an incident occurred. Furthermore, CERT has issued Guidelines for reporting incidents with significant impact on the key service operators and digital service providers,[89] as well as forms for reporting the incidents.[90]

The Cybernetic Security Ordinance regulates in detail measures for obtaining high levels of cybernetic security and prescribed that key service operators are, inter alia, obliged to establish and document the key systems governance policy, establish a risk governance system, continually undertake activities regarding improvements and maintenance of their key systems and conduct incident impact assessments.[91]

Furthermore, controllers must implement a system that provides a timely response to data breaches since, pursuant to the GDPR, supervisory authorities should be notified about a data breach without undue delay and within 72 hours at the latest.[92] In the notification, controllers should describe the nature of the personal breach, likely consequences and measures taken or proposed to address the personal data breach or measures to mitigate its possible adverse effects, and should communicate the name and details of the DPO.[93] Where the personal data breach is likely to result in high risk to the rights and freedom of natural persons, the controller should also notify the data subject.[94]

IX OUTLOOK

The GDPR has evoked significant public attention regarding the field of data protection since it entered into force; the CPDPA is currently overwhelmed by the amount of requested legal opinions and questions regarding the application of current data protection legislation. In addition, to ensure compliance of the national legal framework with the GDPR, new laws and regulations are being considered and more detailed, sector-specific provisions will most probably be adopted in the coming years.

88 Cybernetic Security Act, Article 15.

89 https://www.cert.hr/zks-incident, accessed on 13 July 2019.

90 Cybernetic Security Act, Article 21 and 24.

91 Cybernetic Security Ordinance, Article 6, 9, 10 and 37.

92 GDPR, Article 33.

93 ibid.

94 ibid., Article 34.

Chapter 11

DENMARK

Tommy Angermair, Camilla Sand Fink and Søren Bonde[1]

I OVERVIEW

Similar to other countries in Europe, Denmark has passed legislation designed to supplement the requirements of the EU General Data Protection Regulation (GDPR),[2] which came into force on 25 May 2018. In Denmark the main regulation concerning processing of personal data is the Data Protection Act,[3] which came into force on 23 May 2018.

In addition to the rules of the GDPR, the Data Protection Act and national practice implements certain derogations concerning the processing on personal data, especially in respect of processing of personal data within the employment sector. Furthermore, the national legislation introduces a fourth type of personal data in form of 'confidential' personal data, which may include private, social or economic data concerning the data subject.

It is a well-known fact that few Danish companies worried about data protection compliance or spent significant resources on compliance prior to the entry into force of the GDPR because the fines for non-compliance were low and there was a general lack of awareness and interest in the subject by the public. This was despite the implementation of the EU directive from 1995[4] and the fact that the principal of confidentiality in respect of personal data is a constitutional right.

However, because of the risk of major penalties and commercial risks, such as lack of trust from business partners and other stakeholders, bad publicity in general and loss of goodwill due to personal infringements, many companies invested heavily in compliance projects and programmes in order to be 'GDPR-compliant' before 25 May 2018. Some have even compared the widespread lack of preparedness to the frenzy prior to Y2K at the turn of the millennium.

The ePrivacy Regulation (ePR) is still subject to negotiations in Brussels and will likely be applicable in 2020.

The following chapter provides a pragmatic overview of the current legal situation in Denmark in respect of the national requirements following the GDPR.

---

1 Tommy Angermair is a partner, Camilla Sand Fink is a senior associate and Søren Bonde is an assistant attorney at Clemens.

2 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

3 Act No. 502 of 23 May 2018 on supplementary provisions to the regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

4 European Parliament and Council Directive 95/46/EC 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.

II THE YEAR IN REVIEW

The Danish Act on Processing Personal Data that implemented Directive 95/46 EC came into force in 2002. But despite the fact that the Danish data protection regulation is more than 15 years old, not much attention was paid to data protection in Denmark until the GDPR was passed in 2016. The term 'data protection' was basically unheard of in the general Danish population and in most companies before 2017–2018.

In May 2018, the Danish Chamber of Commerce published an analysis on companies' GDPR compliance costs up to 25 May 2018, which showed GDPR-related costs for the Danish business community of 8 billion kroner.[5] Despite these high costs, most companies have still not completed their basic GDPR compliance projects and many still have not even started their compliance work, even though more than a year has passed since the GDPR came into full force.

The entry into force of the GDPR has thus been the dominant topic over the past year in terms of compliance, and one thing is certain – the term 'data protection' is no longer unknown to private companies, public authorities or the Danish population in general.

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

The rules governing processing of personal data in Denmark are primarily set forth in the GDPR and the Data Protection Act.

In addition, any rules governing processing of personal data in other legislation (*lex specialis*) shall take precedence over the rules laid down in the Data Protection Act (collectively the Data Protection legislation).[6]

In line with the GDPR, the Data Protection legislation applies to the processing of personal data as part of the activities carried out on behalf of a controller or processor established in Denmark, regardless of whether the processing takes place in the EU.

The DPA has published several hands-on guidelines describing how companies must adhere to the Data Protection legislation.[7] The guidelines are not legally binding but they are generally taken very seriously in the public and private sector given the DPA's role as primary regulator and enforcer of the data protection rules in practice.

In connection with personal data set forth in Article 6 of the GDPR, the Data Protection legislation distinguishes between 'regular data' and 'confidential data', which is not explicitly mentioned in the GDPR.

Confidential information is personal data that due to its nature and the context may require 'special protection' as the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to such personal data may cause greater physical, material or non-material damage of the data subject than regular personal data. Depending on the

5 EU's persondataforordning koster danske virksomheder ca. 8 mia. kr. af chefkonsulent Malthe Munkøe og analysekonsulent Jakob Kæstel Madsen, Dansk Erhverv, Maj 2018.

6 Section 1(3) of Data Protection Act.

7 The guidelines are only published in Danish and available at https://www.datatilsynet.dk/generelt-om-databeskyttelse/vejledninger-og-skabeloner/.

circumstances, personal data concerning income and wealth, conditions of employment or internal family relationships may be deemed confidential personal data. The Danish civil registration number (CPR number) is also deemed to be confidential personal data.

Consequently, a controller or processor must take any such precautions needed to safeguard confidential data in accordance with Article 32 of the GDPR.

In addition, confidential personal data will also often be subject to special rules in other regulation as described above.

ii General obligations for data handlers

Controllers are not obligated to register with the DPA in relation to their processing of personal data.

The Data Protection legislation sets forth the fundamental requirements applicable to all processing of personal data. In particular, the Data Protection Act requires that personal data must be collected for specified, explicit and legitimate purposes and may not be further processed in a manner incompatible with those purposes.

To comply with the obligation to notify the data subject in accordance with Articles 12–14 of the GDPR, the controller must take active steps to provide the information. Consequently, it is not sufficient that the relevant information is available on a website or similar, which the data subject is required to find by himself. The form of notification shall reflect the means of collecting personal data. The controller must notify the data subject in writing, unless otherwise accepted by the data subject. Furthermore, the notification shall be provided electronically, if appropriate, for example if the personal data is collected via an electronic form.

If a controller receives unsolicited personal data from a data subject, the controller must notify the data subject in accordance with Article 13 of the GDPR as soon as possible, but, no later than 10 days after receipt.[8]

In accordance with DPA guidelines, a controller must use encryption when transmitting confidential and sensitive personal data by email via the internet. There are usually two possible approaches to achieve this; either encryption is applied to the transport of the data packets containing the email when they are sent over the network (known as TLS encryption), or the content of the email is encrypted by the sender before it is sent over the network. The choice of encryption depends on the characteristics of the personal data to be transmitted and the volume thereof.

iii Data subject rights

The right of access in relation to Article 15 of the GDPR implies that the data subject has the right to receive information concerning the processing of personal data by a controller. The right of access is not limited and includes all information about the processing in IT systems, TV surveillance images, logs, notes, HR information, emails, etc.

The controller may request the data subject to clarify the request for access. However, as a rule the controller may not refuse to comply with the request for access if the data subject refuses to clarify the request.

The controller may derogate from the right of access (and the obligation to notify the data subject of matters concerning Article 13(1)–(3), Article 14(1)–(4) of the GDPR, if the

8 Guideline from the DPA concerning the rights of the data subject, p. 14.

data subject's interest in this information is found to be superseded by essential considerations of public or private interests, including the consideration for the data subject himself, e.g. if a data controller is processing personal data in a whistle-blower inquiry and keeping confidential such personal data is necessary for investigation purposes.

In a recent case, the DPA did not find it contrary to the rules regarding data subjects' right of access to deny access to video surveillance from a public metro station since it was necessary for the security of the metro.[9] In another recent case, the DPA publicly criticised a controller who failed to grant a request for access to TV surveillance showing a father and son in a carwash arguing that it was non-excusable that the controller could not redact other individuals from the surveillance material.[10] Due to the recent cases, the assumption is that exception from right of access has a relatively narrow scope.

In accordance with Article 16 of the GDPR, a controller must correct any inaccurate personal data upon request from a data subject.

However, the situation may arise where a controller does not agree with the data subject that the personal data is inaccurate, for example in a dispute concerning the accuracy of note taking from an HR and employee meeting. The controller is not obliged to correct personal data if the factual belief of the controller is that the personal data processed is accurate.

In such cases, the controller must ensure that a note is made on the disputed information indicating that the data subject does not agree with the accuracy of the personal data, and what the data subject considers to be accurate.

In accordance with Article 17 of the GDPR, a controller must erase personal data at the request of a data subject if the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed.

In a recent case regarding deletion of photos of an intimate nature, the DPA did not find it contrary to the rules not to withdraw and delete published images on the internet, as the DPA assumed that the processing was based on a contract between the parties and not on consent.[11]

In accordance with Article 20 of the GDPR, a data subject has the right to receive and transfer personal data from one controller to another when (1) the processing is done 'automatically' and the processing is based on the consent of the data subject or is required to fulfil a contract and (2) the personal data is provided by the data subject itself.

The term 'provided' shall be interpreted broadly and shall include personal data provided directly by the data subject or collected or generated by the controller, for example, through electronic means. Consequently, personal data a data subject is entitled to receive under Article 20 of the GDPR may include data concerning purchasing behaviour, location data and other observed behaviour. Thus, personal data may include data collected during employment.

The data subject is, however, not entitled to receive personal data that is a result of related processing by a controller, such as the results of processing personal data with an algorithm.

9 DPA case No. 2018-832-0009.

10 DPA case No. 2018-832-0004.

11 DPA case No. 2018-31-0118.

iv Specific regulatory areas

Processing of personal data covered by Article 6(1) and Article 9(1) of the GDPR in an employment context may take place on the basis of consent from the data subject in accordance with Article 7 of the GDPR.[12] However, an employer is – as a rule – allowed to process an employee's personal data to a usual and reasonable extent in connection with the employer's HR administration without obtaining employee consent or DPA authorisation.

Such processing must be justified for operational reasons and may not be offensive to the employee. Furthermore, the controller must inform the employee of the processing no later than six weeks prior to initiation.

In a recent case concerning processing of biometric data (fingerprints), the DPA concluded that the prohibition of processing of personal data under Article 9(1) of the GDPR cannot be waived by reference to Article 9(2)(f) (legal requirements) when processing is carried out as part of the control of an employee's working hours.

The DPA also considered whether processing could be based on employee consent.

Despite this being the general rule, the DPA considered that employee consent to an employer in such matter cannot be considered voluntary and thus cannot constitute a valid basis for processing of biometric data.

When an employee has resigned, his or her email account must be kept active for as short a period as possible. This period is determined by the position and function of the resigned employee and cannot exceed 12 months. In connection with the resignation, an auto-reply must be sent from the email account with notice of the employee's resignation and any other relevant information. The active email account may only be used for receiving emails and forwarding relevant emails internally within the controller's organisation.

If a controller wants to record conversations, for example for quality assurance or for educational purposes, the controller shall – as a rule – obtain consent from the individual involved before the conversation is recorded. In a recent case concerning the use of telephone recordings for training purposes, the DPA issued a temporary order to ban the processing of personal data for internal use, as such processing activities are not within the legitimate interest of the controller.[13] In one case (pre-GDPR), the DPA has specifically stated that storing of telephone recordings from securities trading could take place without consent for documentation reasons. Due to the recent cases from the DPA, the assumption is that the exception has a relatively narrow scope.

Processing of a child's personal data based on consent in connection with the offering of information society services is lawful provided that the child is no younger than 13.

Processing of personal data in connection with healthcare and medical privacy is generally governed by the Danish Health Act.[14] Information to be provided upon request under Articles 15–22 of the GDPR in connection to healthcare and medical privacy must be provided to the data subject without undue delay and in any event within seven days from receipt of the request.

12 Section 12(1) of the Data Protection Act.

13 DPA case No. 2018-31-0977.

14 Act No. 1286 of 02/11/2018.

Television surveillance is governed by rules laid down in the Danish TV Surveillance Act.[15] The term 'television surveillance' means continuous or regularly repeated monitoring of persons by means of a remote or automatic camera. It is irrelevant whether image capture occurs or whether the images are simply displayed on a TV screen or the like.

In particular, a controller must not carry out television surveillance of areas with ordinary traffic.

However, the ban on television surveillance of areas with ordinary traffic does not apply everywhere because of security and crime prevention considerations. The television surveillance prohibition does not for example apply to petrol stations, banks, casinos, hotels and restaurants, shops, etc. Furthermore, television surveillance without image recording of entrances and facades is allowed.

The rules of the Data Protection legislation apply in addition to the TV Surveillance Act.

In addition to the rules on notifying the data subject in accordance with Articles 12–15 of the GDPR, the rule is that the controller conducting television surveillance must clearly indicate that surveillance activities take place by signage or similar.

Recordings containing personal data originating from television surveillance for crime prevention purposes must generally be deleted 30 days after recording.

Together with the general rules of the Data Protection legislation, the rules of the Danish Marketing Act limit the processing of personal data in connection with direct marketing.[16] Direct marketing means when personal data is used to make direct contact with the data subject, for example via email, SMS or a letter.

In particular, a controller may not contact the data subject by use of electronic means for direct marketing purposes unless such processing is based on the consent of the data subject.

A data subject has the right to object to the processing of personal data for direct marketing purposes. If the data subject makes such an objection, the personal data may no longer be used for this purpose. This also applies if a controller performs profiling for marketing purposes.

Irrespective of whether the controller has received an objection from the data subject as described above, it must ensure that the data subject has refused to receive inquiries for marketing purposes. In practice, this is done by verifying whether the registered person appears in the Danish civil registration register (CPR).

Furthermore, a controller is not entitled to disclose or process personal data of a data subject without express consent.

This prohibition does not apply in the case of 'general customer information', which is the basis of categorisation into customer categories, and the interest of the data subject does not exceed the interest of the trader. In this case, the controller must make sure that the consumer has not made inquiries for marketing purposes via the CPR. General customer information does not include detailed information on the data subject's consumption habits, such as information on the data subject's purchase of a car on credit or what goods the data subject has purchased.

15 Act No. 1190 of 11/10/2007.

16 The Danish Marketing Act No. 426 of 03/05/2017.

v Technological innovation

Controllers who make use of big data, the 'internet of things' (IoT), artificial intelligence (AI), facial and body recognition as well as other 'intelligent products' for processing means must assess whether personal data is involved – and, if so, which personal data – for the purposes in question.

Data that may seem innocent at first glance, for example, daily consumption may prove to be personal data, maybe even confidential or sensitive personal data, because the collected data might reveal health-related or private matters.

Consequently, personal data must be classified according to its sensitivity based on the damages and risks from the data subject's perspective in accordance with the GDPR.

The lack of continuity in the solution may result in a personal data threat, for example if a critical healthcare system or surveillance system loses vital personal data or if such data is temporarily unavailable.

Thus, controllers must ensure that the intelligent products can be continuously updated as errors are detected in the software. Therefore, controllers of intelligent products must be aware of the extent to which they rely on external suppliers and require a high security level from them.

In addition to the security and reliability concerns of new IT solutions, the issue regarding ownership and access to personal data developed entirely by automatic algorithms and systems (i.e., AI software) is evident.

Today's AI solutions consist of a series of algorithms that aim to generate an output based on the data it receives. As the amount of data increases, the AI software becomes 'wiser'. Eventually, the AI software can predict accurate output in other similar matters without the use of real data or facts.

In a personal data context, it raises the question 'When is data personal data?', as the data used might not originate from the data subject but from AI software based on its 'experience' gained over time. Similarly, another question arises as to whether this data is accurate enough for the controller to use the personal data in another context, such as for marketing purposes or preventative security solutions.

The GDPR does not provide an answer to these questions, and the DPA is yet to comment on them.

IV INTERNATIONAL DATA TRANSFER AND DATA LOCALISATION

International data transfer is subject to the provisions in the GDPR and as a EU Member State, Denmark is part of the EU–US Privacy Shield.

There are no other restrictions related to international transfer of personal data in the European Economic Area (EEA)[17] other than the restrictions related to national transfers of personal data in the GDPR or special national legislation. According to the GDPR, any transfer of personal data to a third country or international organisations may only take place under specific circumstances and if the conditions in the GDPR, Chapter V, are complied with by the involved controller and the processor. The basic circumstances and conditions are outlined in the following.

17 The European Economic Area includes all EU countries, Iceland, Liechtenstein and Norway.

According to the GDPR, international transfer of personal data to a third country or international organisation may take place without any specific authorisation, 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.

In the time of writing, the European Commission has recognised the following countries as providing adequate protection: Andorra, Argentina, Canada (commercial organisations), the Faroe Islands, Guernsey, Israel, the Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay, and the United States (limited to the Privacy Shield framework).[18]

In the absence of an adequacy decision, a controller or processor may transfer personal data to a third country or international organisation, if the controller or processor has provided appropriate safeguards that enforceable data subject rights and effective remedies are available.

In relation to international data transfers between private companies or organisations it is common that appropriate safeguards are provided by standard contractual clauses or binding corporate rules. Binding corporate rules only include international data transfers between group companies, and application of the rules requires that the competent supervisory authority (DPA) approves the rules. Furthermore, the work related to adopting binding corporate rules is extensive and hence exclusively recommended for large international groups. As opposed to binding corporate rules, standard contractual clauses require no approval from the DPA and may be used to transfer personal data between group companies as well as between external companies.

Furthermore, the standard contractual clauses may be included in other contractual material, such as data-processing agreements or trade agreements provided that no changes are made to the clauses. There are three types of standard contractual clauses, all of which are available on the European Commission's website.[19]

Appropriate safeguards may also be provided between private parties by an approved code of conduct or an approved certification mechanism, both together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards. Such certifications and codes of conducts will probably be important contributions to more transparent access to conduct international data transfers. However, at the time of writing neither codes of conduct nor certifications have been approved in Denmark.

Finally, appropriate safeguards may be provided between private parties by ad hoc contractual clauses between the controller or processor in Denmark and the controller or processor in the third country, subject to DPA approval.

In the absence of an adequacy decision or appropriate safeguards, international transfers of personal data to third countries are restricted to very limited circumstances, including:

a if the data subject has explicitly consented to the proposed transfer after having been informed of the possible risks (except if the activities are carried out by public authorities in the exercise of their public powers);

18 The European Commission's list of approved countries at any given time is available on the European Commission's website: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

19 https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

b if the transfer is necessary for the performance of a contract between the controller and the data subject or the implementation of pre-contractual measures taken at the data subjects requests (except if the activities are carried out by public authorities in the exercise of their public powers);
c if the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person (except if the activities are carried out by public authorities in the exercise of their public powers);
d if the transfer is necessary for important reasons of public interests; or
e if the transfer is necessary for the establishment, exercise or defence of legal claims.

Furthermore, the transfer in question may only take place under the following circumstances:
a if the transfer is not repetitive;
b if the transfer only concerns a limited number of data subjects;
c if the transfer is necessary for the purpose of compelling legitimate interests pursued by the controller that are not overridden by the interests or rights of the data subject;
d if the controller has assessed all the circumstances surrounding the transfer;
e if the controller has informed the DPA of the transfer;
f if the controller has informed the data subject of the transfer and on the compelling legitimate interests pursued (in addition to providing the information referred to in the GDPR, Articles 13 and 14); and
g if the controller or processor reliable for the data transfer has documented the above assessments in the records referred to in GDPR Article 30.

V COMPANY POLICIES AND PRACTICES

To be compliant with the Data Protection legislation, it is essential to know (1) which personal data your company is processing; (2) for how long; (3) why; (4) where the personal data is processed as well as (5) recipients of personal data provided by your company.

The most common measures to obtain essential knowledge of the company's processing activities and to document the company's compliance level are performing a dataflow analysis on a regular basis (e.g., once a year) to keep track of any changing processing activities and preparing a gap analysis indicating any compliance gaps.

It is important to note that GDPR compliance is predominantly based on a basic principle of accountability and the company's individual risk assessments, which means that several measures necessary for GDPR compliance in practice do not follow directly from the GDPR, for example dataflow mapping or ensuring that employees processing personal data have sufficient knowledge of applicable rules and restrictions for processing personal data.

The range of policies and practices required to comply with the GDPR will therefore vary depending on the company's processing activities. The following represents the minimum statutory and non-statutory procedures and documentation regarding private companies' most common general processing activities relating to employee and private customer personal data.

The minimal recommended documentation and procedures regarding all processing activities are as follows:
a documented overview of personal data processed, such as dataflow mapping and gap analysis;

b statutory records of processing activities (Article 30 of the GDPR);

c general privacy policy on websites including statutory information according to the Article s13–14 of the GDPR;

d education of employees, including for example internal guidelines outlining the rules and restrictions of processing personal data in general and regarding the company's specific processing activities (e.g., the use of emails and access rights in IT systems), the company's security measures, how and when to respond to data subject rights requests, and how to identify data breaches etc.; e-learning or other relevant education regarding the processing of personal data; and internal GDPR awareness campaigns etc.;

e cookie policy regarding all websites and technical measures to ensure end user consent to placement of cookies on end user terminal equipment;[20]

f documented assessment of whether or not the company is obliged to designate a data protection officer, if it is questionable whether or not the company is obliged to according to Article 37 of the GDPR;

g statutory private impact assessments regarding high-risk processing activities (Articles 35–36 of the GDPR);

h internal IT and security policy outlining the rules and restrictions of the company's security measures, for example, regarding the use of mobile devices, computers, physical access to buildings or offices, electronic access to IT systems, back-ups, firewalls etc.;

i internal procedures to assess, document and report data breaches. The controller is obligated to register all data breaches internally notwithstanding the company's potential obligation to notify the supervisory authority competent in accordance with Article 33 of the GDPR or communicate the data breach to the data subject in accordance with Article 34 of the GDPR;

j procedures for the erasure of personal data and retention schedules outlining the retention periods for all personal data processed by the controller or processor. There are few rules and guidelines on specific retention periods in Denmark, and most retention periods are set out by the controller's or processor's legitimate purposes to retain the data based on the Danish Limitation Act; Danish legislation on bookkeeping, accounting and tax as well as on DPA case law. Furthermore, the period of limitation for infringement of the GDPR and the Data Protection Act or rules issued in pursuance hereof is five years according to Article 41(7) of the Data Protection Act. The recommended retention periods regarding the most typical processing activities regarding employee and private costumer personal data are set out below; and

k control procedures to ensure the ongoing compliance level, including for example sampling in relation to internal policy compliance and erasure of personal data in accordance with the outlined retention periods, supervision of data processors, controlling and updating the statutory records of processing activities, performing a dataflow analysis on a regular basis, etc.

In addition to the minimum documentation and procedures listed above, the below documentation and procedures are recommended regarding the processing of personal data relating to applicants, present and former employees:

20 Bek nr. 1148 af 09-12-2010 om krav til information og samtykke ved lagring af eller adgang til oplysninger i slutbrugerens terminaludstyr (The Cookie Order) implementing Directive 2002/58/EC (the ePrivacy Directive).

a privacy policy regarding the processing of personal data in the recruitment process including statutory information according to Articles 13–14 of the GDPR;

b procedures for collecting applicant consent for retaining application material for a specific period after the end of recruitment for future relevant vacancies. Retention of the application post-recruitment requires consent from the applicant, except if the purpose for further processing is the defence of a legal claim;

c procedures for erasure of application material after the end of the outlined retention period, which is most commonly a period of six to 12 months from the end of recruitment or time of receipt of unsolicited applications;

d internal privacy policy regarding the processing of HR-related personal information including statutory information pursuant to Articles 13–14 of the GDPR;

e internal guidelines and procedures regarding surveillance, for example, GPS tracking, video monitoring, website logging, mobile device tracking etc.;

f employee consent to process photographs or videos of employees at the company website, social media relating to employees' contact information at the company website and to marketing material, posts, brochures etc.;

g procedures for closing (and erasing) employee email accounts as soon as possible after the end of employment as discussed in Section III.iv; and

h procedures for erasure of the employee's personal file after expiry of the outlined retention period, typically five years after the end of employment based on DPA case law and the limitation period of five years as set out in the Danish Limitation Act regarding claims arising from an employment relationship.

In addition to the minimum documentation and procedures listed above, the following documentation and procedures are recommended regarding the processing of personal data relating to private costumers:

a procedures for collecting consent to approach anyone by means of electronic mail, an automated calling system or fax for the purpose of direct marketing[21] and consent to approach consumers by telephone for the purpose of direct marketing;[22]

b internal guidelines and procedures for collecting and processing personal data in CRM systems;

c procedures and company rules on processing personal data in relation to digital marketing tools, the use of social media etc. (e.g., in relation to Google Analytics, Facebook competitions or inquiries via LinkedIn), especially outlining the rules of international transfer of personal data, the rules for collection consent to publish personal data and the rules in the Danish Marketing Act; and

d procedures on how to give customers the statutory information according to Articles 13–14 of the GDPR if customer calls are recorded (including recording for educational purposes) as discussed in Section III.iv.

21 According to the Danish Marketing Act, Article 10, a trader may not approach anyone by means of electronic mail, an automated calling system or fax for the purpose of direct marketing unless the party concerned has given his or her prior consent.

22 According to the Danish Consumer Act, a trader may not approach consumers by means of telephone for the purpose of direct marketing unless the consumer has given his or her prior consent.

VI DISCOVERY AND DISCLOSURE

Denmark has no general discovery or disclosure scheme in relation to civil litigation corresponding to the rules in countries such as the USA and the UK and it is generally left to each party to decide which information they are willing to provide/introduce into evidence. By operation of the GDPR data subjects now have wider access to their personal data than ever before.

Under the jurisdiction of the GDPR, disclosure of personal data is basically a processing activity equal to all other processing activities. Disclosure of personal data therefore requires a legitimate purpose according to Article 5 the GDPR, and legal grounds according to Article 6 of the GDPR (ordinary personal data), Article 9 of the GDPR (special categories of personal data), the Article 8 of Data Protection Act (personal data about criminal offences) or Article 11 of the Data Protection Act (national identification numbers). The Data Protection legislation equally applies to private companies and public authorities; however, in practice, public authorities' legal basis for processing personal data has a wider scope in special legislation than that of private companies.

If the Danish government or the Danish civil courts request disclosure of personal data in relation to a specific investigation or case, the controller will in practice in most cases have legal grounds for disclosing the data to the government or the civil court if special legislation authorises the government or the civil court to require the disclosure of the personal data in question (e.g., Sections 298(1) and 299(1) of the Danish Administration of Justice Act[23] according to which the court may order disclosure of documents relating to the matters in question). If the Danish government or the Danish civil courts do not have legal grounds to request disclosure of the personal data, the controller must have other legal grounds for disclosing the personal data in the Data Protection legislation. The controller may, for example, disclose information regarding national identification numbers 'if the disclosure is a natural element of the ordinary operation of enterprises etc. of the type in question and the disclosure is of decisive importance for unique identification of the data subject or the disclosure is demanded by a public authority' according to the Data Protection Act, Article 11(3). This legal basis may for example be used by real estate agents and lawyers in relation to their disclosure of the parties' national identification numbers to the Danish registry when applying for registration of documents regarding property transactions.

The processor may also disclose personal data about criminal offences 'if the disclosure takes place to safeguard private or public interests which clearly override the interests of secrecy, including the interests of the person to whom the data relates' according to Article 8(2) of the Data Protection Act. This legal basis may, for example, be used by an employer in relation to its disclosure of personal data about an employee's criminal offence to the police as part of an investigation regarding the employee.

In relation to disclosure of requests or demands from foreign prosecutors, courts or governments, the above-mentioned GDPR rules on international transfer of personal data also apply if a foreign government requests the disclosure of personal data stored under the jurisdiction of the GDPR.

Especially with regards to the US government disclosure requests to US-based organisations storing personal data under the jurisdiction of the GDPR or the former

23 Lov 2018-11-14, nr. 1284 Retsplejeloven (the Danish Administration of Justice Act).

Directive on the protection of personal data,[24] the legal situation may cause major conflicts for US-based organisations obligated to disclose the data in question under US law and prohibited from disclosing the data in question under European law. After the enforcement of the US CLOUD Act,[25] which essentially provides that the obligation for organisations under the US jurisdiction to comply with US law enforcement agencies' search warrant to gain access to data regardless of whether data in question is located within or outside the United States, the legal state regarding transfer of personal data from EU to the United States is still uncertain although the US CLOUD Act to some extent tries to deal with the above mentioned conflicts, for example, by stating that any disclosure of data must adhere to local law.

The leading case in question between the New York Prosecution Agency and Microsoft regarded a legal demand for Microsoft to disclose data located on servers in Ireland, which Microsoft refused, because the disclosure would constitute an infringement of the Irish data protection regulation. The case was dismissed by the US Supreme Court after the enforcement of the CLOUD Act, but though dismissed the dispute is still not settled and it is expected that a new case between the parties will be settled according to the CLOUD Act. If the US government succeeds in the new case, controllers under the jurisdiction of the GDPR cannot be certain that US-based data processors (such as Microsoft or Apple) can actually comply with the rules of international transfer of personal data and disclosure in the GDPR, because they may be forced to disclose personal data regarding European citizens to the US government regardless of the rules in the GDPR or – as far as Denmark is concerned – the Data Protection Act.

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

Based on the Data Protection legislation, the DPA is essentially the only enforcement agency with regards to data protection and privacy in Denmark with one minor exception (according to the Danish Act on Data Protection regarding supply of public electronic communications services,[26] the Danish Business Authority is the primary enforcement agency when it comes to security issues and security breaches in the telecommunications and internet sector).

According to the Data Protection Act, the DPA has several investigatory powers. The DPA may, for example, request access to any information relevant for its activities, including for the decision of whether a particular matter falls within the provisions of the Data Protection legislation. Furthermore, DPA staff must at any time – against satisfactory proof of identity but without a court order – be given access to all premises from where a processing activity is carried out, including any data processing equipment. If required, the police will help to secure access. The DPA therefore has the authority to audit private companies and public authorities – announced as well as unannounced – and conduct investigations of the controller's or processor's adherence to the Data Protection legislation.

24 The European Parliament and Council Directive 95/46/EC 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.

25 The Clarifying Lawful Overseas Use Of Data Act, 23 March 2018 (The U.S. CLOUD Act).

26 Bek. nr. 462 af 23. maj 2016 om persondatasikkerhed i forbindelse med udbud af offentlige elektroniske kommunikationstjenester.

Before the GDPR came into force, the DPA also had investigatory powers, including audits, but these powers was utilised to a much lesser extent than today. In 2017, the DPA held 73 audits and in 2018, where the GDPR came into force, the DPA held 329 audits.[27] Both numbers include planned written and physical audits and raids. After the GDPR came into force, the DPA's audits have increased substantially, and the DPA has now announced a number of planned written and physical audits regarding different business areas and different data protection subjects twice a year. For example, the DPA plans to audit two law firms, one accountancy firm and one union regarding the encryption of emails, and three public authorities and three private companies regarding compliance with the data subject access rights.[28] Furthermore, the DPA is planning a number of audits based on the DPA's own initiative, complaints etc., but it seems that such audits also are notified to the controller or processor being audited prior to the audit. The DPA has not published the number of actual raids or unannounced audits after the GDPR came into force, but it seems to be quite few if any at all.

According to Article 58 of the GDPR, the DPA also has a number of corrective and sanctioning powers, including the power to issue warnings about intended processing operations likely to infringe the Data Protection legislation; to issue reprimands where processing activities have infringed the Data Protection legislation; to order processing operations brought into compliance with the GDPR and to impose temporary or definitive limitations including bans on processing activities.

The Danish legal system does not provide for administrative fines, which means that the processing activity infringing the Data Protection legislation is reported to the police by the DPA with an indicated fine, after which the prosecution will build a case against the defendant. The procedure is subject to the general rules of criminal procedure set out in the Danish Administration of Justice Act, which governs all aspects of civil and criminal proceedings. In Denmark, any fine for infringement of the Data Protection legislation is therefore imposed by the courts of Denmark.

Private companies and persons infringement of the GDPR (and the Data Protection Act) is subject to fines 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, whichever is higher, regarding among other things infringement of the provisions regarding children's consent in relation to information society services (GDPR, Article 8), Data protection by design and by default (GDPR Article 25) and codes of conduct and certification (GDPR, Articles 41–43).

Private companies and persons infringement of the GDPR (and the Data Protection Act) is subject to fines 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, regarding among others infringement of the provisions regarding the basic principles and legal grounds (GDPR Articles 5–7 and 9), data subject rights (GDPR, Articles 12–22), international transfer of personal data (GDPR, Articles 44–49) and the Data Protection Agency's corrective orders (GDPR, Article 58).

Any infringement of the Data Protection legislation by Danish public authorities and institutions is subject to a fine of up to 4 per cent of the annual operating grant up to a maximum of 16 million kroner.

27 Datatilsynets årsrapport 2018, page 10.

28 The DPA's published audit plans for the first half of 2019: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2019/jan/planlagte-tilsyn-i-foerste-halvaar-af-2019/.

The DPA registered 12,205 cases in 2018, including hearings regarding the drafting of laws and executive orders of importance for the protection of privacy, investigations, audits, security breaches and international cases, as opposed to 5,024 registrations in 2017.[29]

Data protection and privacy did not have great importance in Denmark before 25 May 2018, and the most obvious reason for this is without a doubt that infringement of the data protection regulation was subject to none or hardly any sanctions pre-GDPR. This is emphasised by the fact that the highest fine issued in Denmark prior to 25 May 2018 was 25,000 kroner.

It is safe to say that post-GDPR, data protection has been taken seriously by Danish companies and public authorities, which is largely as a result of the DPA's increased activities as discussed above. In 2019, the DPA has issued a series of reprimands, bans and warnings, and in two cases the DPA has reported a private company to the police for infringement of the GDPR with indicated fines of 1.5 million and 1.2 million kroner respectively, both regarding infringement of Article 5(1)(e) of the GDPR, because said companies stored personal data for longer periods than necessary for the purposes for which the data was processed.

ii Recent enforcement cases

The most significant recent cases are the above-mentioned cases, which are the first data protection enforcement cases in Denmark.

The first case relates to a taxi company that had stored approximately 9 million collection and drop-off points linked to customer telephone numbers that could therefore be linked to specific people. The taxi company had attempted to anonymise the information by erasing customer names and argued that a longer retention period regarding the telephone numbers was necessary for business development purposes and that telephone numbers were 'the key to the database'. The DPA stated that the taxi company had no legitimate purpose for the separate retention period regarding telephone numbers, and that a controller or processor cannot base a processing activity's purpose on the fact that a system makes it difficult to comply with the GDPR. The DPA reported the infringement to the police with an indicated fine of 1.2 million kroner.

The second case relates to a retail company that had stored personal data regarding approximately 385,000 private customers in a primarily phased system without setting a retention period for the data in question. In this case, the DPA has reported the infringement to the police with an indicated fine of 1.5 million kroner.

Both cases are based on DPA planned audits, and the indicated fines will – if sanctioned by the court – be the highest fines ever imposed in Denmark regarding a data protection infringement.

Neither case has been settled by the Danish district court, and due to their public importance, it is expected that both cases will be appealed to the Danish High Court and possibly even to the Danish Supreme Court.

In other cases, the DPA has refrained from reporting infringements to the police, even though the infringement appeared to be of the same nature as those mentioned above. The DPA has instead issued reprimands, ordered a processing activity to be brought into compliance with the GDPR or imposed temporary or definitive limitations on processing activities. The DPA, for example, imposed a temporary ban on one of Denmark's largest

29 The DPA's annual report for 2018, page 10.

telecommunication companies for recording costumer calls without customer consent, even though the reason that the company did not collect costumer consent was that their system did not support this. The number of customer call recordings without legal grounds has not been published, but it seems that the nature of this infringement is at least as serious as the above-mentioned cases resulting in a police report.

Looking generally at the DPA's post-GDPR practice, it is still very difficult to deduce any guidance revealing which infringements will result in a police report with an indicated fine and a subsequent criminal case, and which infringements will entail less severe sanctions, such as a ban or a reprimand. However, it is hope that this will become clear in the years to come, when more criminal cases have been settled and DPA sanctions have been imposed.

iii Private litigation

According to Article 82 of the GDPR, any person who has suffered material or non-material damage as a result of an infringement of the GDPR (or the Data Protection Act) shall have the right to receive compensation for the damage suffered. In many cases, private persons have insurance that covers legal expenses related to lawsuits, and there are almost no other options for free legal aid in Denmark. Private lawsuits regarding data protection are not common in Denmark, neither before nor after the GDPR came into force. Furthermore, Denmark has no tradition for pursuing claims by class action, which was first legalised in Denmark in 2008.

Due to the significantly increased public awareness regarding data protection post-GDPR, we may see more lawsuits where private individuals seek recovery (e.g., regarding data breaches or infringement of data subject rights). Nonetheless, an important basic principle of Danish law on damages is that a claim for damages can only cover the plaintiff's actual loss. In special cases – primarily criminal offences – the plaintiff may seek a special compensation (tort law) in addition to damages. According to Danish case law and the Danish Liability for Damages Act, a plaintiff may claim such compensation in cases regarding data protection; however, awarded amounts so far have been relatively small. Pre-GDPR, Danish courts awarded amounts of 5,000–25,000 kroner of compensation. No civil lawsuits have been settled in Denmark post-GDPR, but it is not expected that Danish courts will increase compensation amounts in future, mainly because compensation is regulated by the Danish Liability for Damages Act as opposed to the Data Protection legislation. It is thus likely that we will see more class actions in future, because the costs of a civil lawsuit in practice will be significantly higher than the potential compensation.

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

There are no requirements for private controllers to store personal data exclusively in-country. Bookkeeping materials can be retained abroad but must be physically available in Denmark to a certain extent. The Danish Minister of Justice may, however, lay down rules to the effect that any personal data processed in specified IT systems and kept for public administrative authorities, must be stored, in full or in part, exclusively in-country. No such rules are in effect at the time of writing.

There is no general requirement from the government to access software or decryption codes. However, prior to the publishing of this book, a new law regarding cybersecurity was adopted. The law has been widely criticised as IT companies and experts believe that the law confers too much power on the National Center for Cybersecurity (CFCS).

The CFCS is part of the National Intelligence Service and is responsible for detecting, analysing and helping to address security incidents at affiliated authorities and private businesses.

Under the new law, the CFCS may, in special cases, require companies of special social importance and regions and municipalities to be connected to the network security service for the purpose of monitoring network communication. The order can only cover parts of the company, region or municipality with significant impact on Denmark's critical infrastructure.

Furthermore, the CFCS may process data in transmission (e.g., when the data is sent outside the organisation) or when it is stored locally on servers in the country from affiliated authorities and companies without a court order to support a high level of information security in society. Affected companies may be operators of drinking water supply and distribution, energy (electricity, oil and gas), transport, banking, health and financial and digital infrastructure, whereas online market operators, online search engines or cloud services are not considered to be critical infrastructure.

IX CYBERSECURITY AND DATA BREACHES

Denmark ranks seventh in the latest update of the international National Cybersecurity Index (NCSI).[30]

The NCSI is developed and maintained by the Estonian e-Governance Academy. The ranks are calculated based on 46 indicators within three main categories: 'general cyber security indicators', 'basic cyber security indicators' and 'event and crisis management indicators'.

The high ranking is primarily due to the fact that Denmark has implemented the EU Directive on Network and Information Security (NIST), which includes several security requirements and a notification obligation in case of security incidents.

Consequently, security breaches relating to personal data or other security events relating to significant parts of Denmark's infrastructure, for example supply, digital infrastructure, finance and telecommunications shall be reported to the relevant authorities.

In relation to information privacy standards, the ISO/IEC 27001 framework on information security is mandatory for all government and public authorities.

In relation to private companies, Section 115 of the Danish Companies Act stipulates that the board of directors of a capital company among other things must ensure that the company has an overview of the risks related to IT facilities within the company and that IT facilities are robust and reliable. Apart from this, no Danish laws lay down cybersecurity requirements (beyond the GDPR) to cover corporate networks, proprietary data, availability and integrity of business data.

In addition to the ISO/IEC 27001 framework, the SANS CIS Risk Assessment Method, SANS CIS Critical Security Controls or ISO/IEC 27005 on Information Technology – Security Techniques – Information Security Risk Management are generally used in relation to privacy and cybersecurity compliance.

30 https://ncsi.ega.ee/.

X OUTLOOK

The GDPR has probably had more effect on Danish society in general, including the Danish business community and public authorities, than any other law ever implemented in Denmark. Most companies still have comprehensive compliance work ahead, and many have still not commenced their compliance work even though more than one year has now passed since the GDPR came into force. In the years to come, DPA sanctioning and the pending criminal cases in Denmark as well as in Europe will form applicable case law and guidelines, both regarding the sanctioning level and, for example, specific retention periods; the extent of the legal grounds in the Data Protection legislation and will hopefully answer many of the unanswered key questions arising from the GDPR.

Chapter 12

GERMANY

Olga Stepanova and Florian Groothuis[1]

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 to meet the requirements of a society in which data processing has grown 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). Whereas the GDPR has been applicable from 25 May 2018, the ePrivacy Regulation is still subject to negotiations at the European level and will probably be applicable in 2022. 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.

1 Olga Stepanova is an associate and Florian Groothuis is a scientific researcher at Winheller Rechtsanwaltsgesellschaft mbH.

II THE YEAR IN REVIEW

The past year was characterised by compensating for the legal uncertainty caused by the new provisions of the GDPR. For this, the German data protection authorities published several working papers to give companies guidance on adjusting to the new data protection rules. Although the GDPR is directly applicable and does not have to be implemented into national law, it contains numerous 'opening clauses' so Member States can introduce additional national provisions to concretise provisions of the GDPR for specific issues (e.g., in connection with employees) within its legal framework.

The German legislator used this leeway and adopted a Data Protection Adaption Act which introduced in particular a new version of the BDSG and is applicable since the 25 May 2018. A second Data Protection Adaption Act is in the legislation process and focuses primarily on changes in area specific laws. Also it aims to modify the threshold from when data controllers and processors are obliged to designate a data protection officer from 10 to 20 persons being constantly employed in automated data processing activities.

Before the GDPR went into force, the mass media often reported about the high fines Data Protection Authorities (DPAs) are authorised to impose when infringements occur. In case of serious data protection violations the DPAs can indeed impose fines of up to €20 million or 4 per cent of annual global turnover, whichever is higher. However, the German DPAs acted rather restrained so far when sanctioning violations.

iii Basics

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, even after the regulation has been applicable for several months.

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.

Since the GDPR has tightened the requirements for obtaining valid consent to process personal information, in practice, the relevance of the consent as legal basis has decreased and shifted to the legitimate interest of the data controller. 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 DPAs, 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 in order 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. For minimizing the uncertainty whether a PIA should be performed the German DPAs issued 'blacklists' that contain processing activities that always require a PIA.[2]

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.

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 in March 2019, 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. That is why a lot of websites needed to amend not only their privacy policy, but also the cookie settings, so that i.e. for analysis cookies a consent under the strict rules of GDPR needs to be obtained.

ii General obligations for data controller

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 controller may collect and use personal data only to the extent that the law specifically permits pursuant to Article 6 GDPR.

One relevant legal basis is still the consent according to Article 6 (1) (a) GDPR which 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 withdraw 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.

As mentioned before, the focus to justify data processing activities has shifted towards the legitimate interest basis pursuant to Article 6 (1) (f) GDPR. For this, the data controller must perform a three-part test and identify the legitimate interest, explain the necessity of achieving it and balance the interest against the data subject's interests, rights and freedoms.

2 https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/HBDI_Verarbeitungsvorg%C3%A4nge%20-Muss-Liste%20Berlin%20%28002%29.pdf.

As long as the data subject would reasonably expect the respective processing activities and they have a minimal impact on the individual's privacy, no consent is needed. However, similar to the consent, the data subject has the right to object to processing activities based on the legitimate interest at any time according to Article 21 (1) GDPR. The important difference is that the data controller may continue its processing activities despite the data subject's objection when the data controller can demonstrate compelling legitimate grounds which override the individual's interests, rights and freedoms.

Moreover, personal data may only be collected for specified purposes the data controller has determined before the collection took place. They must not be used for secondary purposes that are incompatible with the collection purpose. When verifying the compatibility between the primary collection and the secondary processing purpose, the criteria named in Article 6 (4) GDPR are of paramount importance.

For ensuring the transparency of data processing activities the data controller is obliged according to Articles 13 and 14 GDPR, inter alia, to inform the user of the extent and purpose of the processing of personal data. Although the DPAs in Germany were hesitant in the beginning to allow a layered approach in providing the legally prescribed information, a change is emerging. Regarding video surveillance the German Data Protection Conference permits the distribution into essential information that must be provided onsite and other information that can be looked at online.[3] Single DPAs follow the layered approach as suggested by the European Data Protection Board in general.[4]

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 monitor the behaviour of data subjects on the internet and create user profiles. Thus, an

3 DSK, Kurzpapier Nr. 15, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_15.pdf.

4 LDA Bayer, 8. Tätigkeitsbericht, https://www.lda.bayern.de/media/baylda_report_08.pdf#page=45; EDPB, Working Paper 260, https://datenschutz-hamburg.de/assets/pdf/wp260rev01_en.pdf.

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).[5]

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 all the requirements of the GDPR, 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 that processing has to be transparent and the controller shall be responsible for obeying this principle.

An important part of the transparency principle is providing understandable information about the division of roles when involved parties are processing personal data, as the ECJ on Facebook fanpages has shown (ECJ, 5 June 2018 – C-210/16). In this case the ECJ stated that the fanpage operator and Facebook are acting as joint controllers. 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 fanpage operators receive the visitor's user data (even if 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 fanpage 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 fanpage operators are still joint controllers.

Facebook reacted and published a Page Insights Controller Addendum to fulfil the requirements established by the ECJ regarding joint controllership. Nevertheless, the German Data Protection Conference found these adjustments insufficient and therefore in violation of the GDPR. In particular, Facebook grants itself the sole decision-making power in respect of the processing of insights data and this is in conflict with the joint controllership pursuant to Article 26 GDPR. Furthermore, Facebook does not describe the processing activities regarding the fanpage in a transparent way.[6]

While the ECJ confirmed its findings in respect of the joint controllership in the Jehovah's Witnesses decision (ECJ, 10 July 2018 – C-25/17), they will be relevant in another dispute before the ECJ involving Facebook. The Düsseldorf Higher Regional Court has asked the ECJ, inter alia, whether a German online retailer that includes the 'Facebook Like' button

5 DSK, Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf.

6 DSK, Positionierung zur Verantwortlichkeit und Rechenschaftspflicht bei Facebook Fanpages, https://www.datenschutzkonferenz-online.de/media/dskb/20190405_positionierung_facebook_fanpages.pdf.

on its website is a joint controller alongside Facebook. The Advocate General confirmed joint controllership and set a low threshold for assuming joint controllership (Opinion of Advocate General Bobek, 19 December 2018 – C-40/17).

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 'adequacy decision' that these countries ensure an appropriate 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, Japan, 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:

a the data subject has given his or her consent;

b 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;

c 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;

d the transfer is necessary for important reasons of public interest;

e the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims;

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

g 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.

iii Brexit

The free flow of data between EU Member States and the United Kingdom (UK) depends whether the UK and the EU can reach a deal that covers data protection before the UK leaves the EU. Since the Commission has declined to start the process of assessing the UK's level of data protection and declaring it for adequate, a 'hard' Brexit would have a severe impact on the unhindered data exchange between the EU and the UK. In such scenario, the UK would be treated from a data protection point of view as third country equivalent to India. Therefore, personal data could only be transferred to the UK when companies have implemented the above-mentioned safeguards, namely standard contractual clauses and 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 authorised to supervise the data privacy compliance of state entities, as well as all non-public entities whose principal place of business is established in the particular 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, which are often suspected of processing data in an unlawful way, and can be used as sharp sword to ensure conformity with GDPR. Especially the dynamic and the dependency on the turnover aims to achieve a deterrent effect even on the most be wealthiest companies worldwide.

However, fines amounting to millions, as feared by companies, have not yet been imposed by the German DPAs. The DPA of the federal state of Baden-Württemberg imposed a fine of €80,000 because health data were accidently published on the internet. In another case a bank was fined €50,000 by the DPA of the federal state of Berlin for processing personal data of former clients without legal grounds.

Mostly infringements are caused by insufficient 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 Information obligations in context of private litigation

The GDPR obliges the data controller to provide the data subject with certain information about the data processing (see Articles 13 and 14 GDPR). It must inform the data subject about 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 its legal basis, the source of the data, where applicable, to whom they are disclosed, the duration of processing and the retention policy. Additionally, the data subject must 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 clearly shows that the data subject is being given numerous rights, but also that the controller will have to invest more effort in satisfying the requests in a proper way, which is a question of time and expense.

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. In particular, damages for pain and suffering from data protection violations can be claimed under civil law.

In Germany, the DPAs are not necessarily involved in enforcing the rights of individual data subjects. Instead, complaints against domestic controllers can 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 upon.

VI CONSIDERATIONS FOR FOREIGN ORGANISATIONS

As data protection gradually becomes a question 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. 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 not fully understood and often only can be understood by a teleological interpretation. In Germany, there are 16 DPAs that follow slightly different interpretations of the GDPR legislation. 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 the report of the Commission on the evaluation and review of the GDPR that is due by 25 May 2020 and what impact the GDPR will have on companies until then, especially on social media operators.

Chapter 13

HONG KONG

Yuet Ming Tham[1]

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 2018 to June 2019. 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,[2] the April 2016 Revised Code of Practice on Human Resource

1 Yuet Ming Tham is a partner at Sidley Austin LLP.

2 www.pcpd.org.hk/english/resources_centre/publications/files/DataBreachHandling2015_e.pdf.

Management,[3] the April 2016 Privacy Guidelines: Monitoring and Personal Data Privacy at Work[4] and the June 2016 guidance note on Proper Handling of Data Access Request and Charging of Data Access Request Fee by Data Users.[5] 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:

a 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);[6]

b 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);[7] and

c 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).[8]

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.[9] Additionally, the PCPD released revised Guidance on CCTV Surveillance and Use of Drones.[10]

From mid-2018 to mid-2019, Hong Kong and Singapore signed a memorandum of understanding (MOU) to strengthen cooperation in personal data protection at the 51st Asia Pacific Privacy Authorities Forum. The MOU was signed by Mr Stephen Kai-Yi Wong (the PCPD) and Mr Yeong Zee Kin (Deputy Commissioner of Singapore's Personal Data Protection Commission). Stemming from this cooperative MOU, Hong Kong and Singapore jointly released a Guide to Data Protection by Design for ICT Systems on 31 May 2019.[11] The PCPD also released the revised Guidance on Data Breach Handling and the Giving of Breach Notifications[12] and the March 2019 Revised Privacy Management Programme: A Best Practice Guide.[13]

The PCPD reported that it had received 1,890 complaints in 2018, which included 139 complaints relating to the leakage of passengers' personal data by Cathay Pacific Airways.

3 www.pcpd.org.hk/english/data_privacy_law/code_of_practices/files/PCPD_HR_Booklet_Eng_AW07_Web.pdf.

4 www.pcpd.org.hk/english/data_privacy_law/code_of_practices/files/Monitoring_and_Personal_Data_Privacy_At_Work_revis_Eng.pdf.

5 www.pcpd.org.hk/english/resources_centre/publications/files/DAR_e.pdf.

6 www.pcpd.org.hk/english/resources_centre/publications/files/DataBreachHandling2015_e.pdf (The publication on the PCPD website has not yet been updated).

7 www.pcpd.org.hk/english/resources_centre/publications/files/GN_CCTV_Drones_e.pdf.

8 www.pcpd.org.hk/english/resources_centre/publications/files/dcr_e.pdf.

9 www.pcpd.org.hk/english/resources_centre/publications/files/electioneering_en.pdf.

10 www.pcpd.org.hk/english/resources_centre/publications/files/GN_CCTV_Drones_e.pdf.

11 www.pcpd.org.hk//english/resources_centre/publications/files/Guide_to_DPbD4ICTSystems_May2019.pdf.

12 www.pcpd.org.hk//english/resources_centre/publications/files/DataBreachHandling2015_e.pdf.

13 www.pcpd.org.hk//english/resources_centre/publications/files/PMP_guide_e.pdf.

The 1,890 complaints represent a 23 per cent increase from the 1,533 complaints in 2017 (excluding the 1,968 complaints relating to the reported loss of laptops containing personal data of election committee members and electors by the Registration and Electoral Office in 2017 (REO Incident)). Most of the complaints involved were made against private sector organisations with financial, property management, and transportation companies leading the way. Twenty-seven per cent of the complaints related to use of personal data without consent and approximately25 per cent complaining about the purpose and manner of the data collection. The PCPD received 501 ICT-related privacy complaints in 2018, representing a more than double increase (111 per cent) as compared to 2017. Most of these complaints related to the disclosure or leakage of personal data on the Internet and through social networking websites. The PCPD received notice of 129 data breach incidents in 2018 compared to 106 incidents in 2017 (excluding the REO Incident), representing an increase of 22 per cent as compared to 2017. The number of direct marketing complaints remained relatively flat (181 complaints in 2018, comparable to 186 complaints in 2017).[14]

With respect to enforcement in 2018, the PCPD issued 16 warnings as compared to 26 warnings in 2017. No enforcement notice was issued in 2018 as compared to three enforcement notices in 2017. Referrals of cases for criminal prosecutions to the police fell from 19 in 2017 to six in 2018, all of which involved direct marketing violations. The number of actual prosecutions slightly decreased from four in 2017 to two in 2018. Both prosecutions in 2018 concerned direct marketing violations, which resulted in convictions. In January 2018, PARKnSHOP pleaded 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.[15] In August 2018, Hutchison Telecommunications pleaded guilty to two charges under the PDPO, both of which related to direct marketing violations, resulting in a total fine of HK$20,000.[16]

The PCPD does not systematically publish decisions or reports based on the outcome of its investigations. For the entirety of 2018 and up until June 2019, the PCPD published two investigation reports (one on the unauthorised access to personal data of passengers by Cathay Pacific Airways Limited and Hong Kong Dragon Airlines Limited,[17] and the other on the personal data leakage accident of Hong Kong Broadband Network Limited).[18] The PCPD also published an inspection report in December 2018, offering recommendations to private tutorial institutions in strengthening the data protection in the private tutorial industry.[19] Additionally, the PCPD published a compliance check report in April 2019 regarding the personal data collection in shopping mall membership programmes and online promotion activities, recommending the practice of minimum collection of personal data.

14 www.pcpd.org.hk/english/news_events/media_statements/press_20190131.html.

15 www.pcpd.org.hk/english/news_events/media_statements/press_20180102b.html.

16 www.pcpd.org.hk/english/news_events/media_statements/press_20180822.html.

17 www.pcpd.org.hk/english/enforcement/commissioners_findings/investigation_reports/files/PCPD_Investigation_Report_R19_15281_Eng.pdf.

18 www.pcpd.org.hk/english/enforcement/commissioners_findings/investigation_reports/files/PCPD_Investigation_Report_R19-5759_Eng.pdf.

19 www.pcpd.org.hk/english/enforcement/commissioners_findings/inspection_reports/files/IR_E_R18_13069.pdf.

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.[20] 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, among others, the Telecommunications Ordinance, the Theft Ordinance and the Crimes Ordinance.[21] According to the Hong Kong police, there were 7,838 computer crime cases in 2018, with an associated loss of HK$2.8 billion as compared to 5,567 cases in 2017 amounting to a loss of HK$1.4 billion.[22]

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. In December 2016, the HKMA announced implementation details of its Cybersecurity Fortification Initiative undertaken in collaboration with the banking industry[23] as well as launching an industry-wide Enhanced Competency Framework on Cybersecurity.[24] In October 2017, the SFC published the Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading (the Guidelines),[25] and issued two circulars to licensed corporations engaged in internet trading, one on good industry practices for IT risk management and cybersecurity;[26] the other on the implementation of the Guidelines.[27] In May 2018, SFC issued a circular to intermediaries on receiving client orders through instant messaging.[28] In January 2019, the HKMA issued the Update on Enhanced Competency Framework on Cybersecurity.[29]

iii 2019 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.

20 www.police.gov.hk/ppp_en/04_crime_matters/tcd/legislation.html.

21 www.infosec.gov.hk/english/ordinances/corresponding.html.

22 www.infosec.gov.hk/english/crime/statistics.html.

23 www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2016/20161221e1.pdf.

24 www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2016/20161219e1.pdf.

25 www.sfc.hk/web/EN/assets/components/codes/files-current/web/guidelines/guidelines-for-reducing-and-mitigating-hacking-risks-associated-with-internet-trading/guidelines-for-reducing-and-mitigating-hacking-risks-associated-with-internet-trading.pdf.

26 www.sfc.hk/edistributionWeb/gateway/EN/circular/intermediaries/supervision/doc?refNo=17EC74.

27 www.sfc.hk/edistributionWeb/gateway/EN/circular/intermediaries/supervision/doc?refNo=17EC72.

28 www.sfc.hk/edistributionWeb/gateway/EN/circular/intermediaries/supervision/doc?refNo=18EC30.

29 www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2019/20190110e1.pdf.

In June 2019, the PCPD received 130 complaints and enquiries relating to 'doxxing'[30] of police officers, their friends and relatives, and 36 complaints and enquiries relating to suspected unauthorised transfer of patients' data to the police by medical staff, along with Hospital Authority's notification on suspected data leak of its accident and emergency information system (the A&E incident). The PCPD has commenced a compliance check on the Hospital Authority.

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;

30 Doxxing refers to an internet-based practice of researching and broadcasting private or identifiable information about an individual or organisation.

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.[31] 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. On 9 April 2019, the Hong Kong Commerce and Economic Development Bureau announced a plan to amend the UEMO to extend the regulatory framework to cover direct person-to-person telemarketing calls, including by establishing a new do-not-call register, and imposing fines and imprisonment on violators. The specific timetable for the proposed legislative amendments is yet to be announced.

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.[32] 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.[33] The court fined the company HK$10,000.

31 Report on Further Public Discussions on Review of the Personal Data (Privacy) Ordinance (April 2011).

32 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.

33 www.pcpd.org.hk/english/news_events/media_statements/press_20150914.html.

Additional convictions and fines followed in 2016 and 2017 for direct marketing violations. The most recent cases initiated by the PCPD resulting in fines and convictions were a June 2019 guilty plea by KOA International Limited, a beauty product company, for failing to take specified actions and obtain customer's consent before using her personal data in direct marketing, resulting in a HK$8,000 fine,[34] and a May 2019 guilty plea from an auction company that failed to take specified actions and obtain consent before using the data subject's personal data and failed to inform the data subject of her rights under the PDPO to request for not using her personal data in direct marketing without charge, resulting in a HK$20,000 fine.[35] 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.

iii Technological innovation and privacy law

Search engines, cookies, online tracking and behavioural advertising

While there are no specific requirements in Hong Kong regarding the use of search engines, 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. Privacy-enhancing technologies should be adopted to minimise the risk of personal data exposure, such as encryption or hashing to maintain data confidentiality, robots exclusion protocol to prevent search engines from indexing websites, anti-robot verification to stop databases from being downloaded in bulk by automation.

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.

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 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,

34 www.pcpd.org.hk/english/news_events/media_statements/press_20190618.html.

35 www.pcpd.org.hk/english/news_events/media_statements/press_20190527.html.

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.

Fintech

In March 2019, the PCPD published an information leaflet entitled 'Tips for Using Fintech', which offers advice to users in protecting their personal data privacy in the use of fintech and recommends good practices for fintech providers or operators.[36] In May 2019, the HKMA issued a circular on the Use of Personal Data in Fintech Development to encourage authorised institutions to adopt and implement the Ethical Accountability Framework (EAF) for the collection and use of personal data issued by the PCPD.[37] The EAF promotes ethical and fair processing of data through (1) fostering a culture of ethical data governance; and (2) addressing the personal data privacy risks brought by emerging information and communication technologies such as big data analytics, artificial intelligence and machine learning.

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.

36 www.pcpd.org.hk/english/resources_centre/publications/files/fintech.pdf.

37 www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2019/20190503e1.pdf.

The PCPD published an information leaflet in April 2019 entitled 'Data Ethics for Small and Medium Enterprises' to advise small and medium-sized enterprises (SMEs) on the core values of data ethics including respectful, beneficial and fair, and the adoption of the ethical data impact assessment before pursing any advanced data processing activity.[38]

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.

Notwithstanding the above, in response to the A&E incident, the PCPD stressed that hospitals should first ask the enforcement authority requesting personal data to provide sufficient information, including but not limited to the purpose of data collection, the nature of the case being investigated and the relevance of the requested data to the investigation. The enforcement authority also has the duty to inform the hospital whether the supply of data is obligatory, or else the enforcement authority may be considered to contravene the PDPO through misleading the hospital or on abuse of power grounds.[39]

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.

38 www.pcpd.org.hk/english/resources_centre/publications/files/dataethics_en.pdf.

39 www.pcpd.org.hk/english/news_events/media_statements/press_20190623.html.

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

i 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,[40] the Crimes Ordinance[41] and the Theft Ordinance,[42] 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.

The Hong Kong Monetary Authority announced in January 2019 that the financial sector will be stepping up its efforts to combat cybercrime through the Cyber Resilience Assessment Framework (C-RAF), which is a three-part assessment instrument that helps artificial intelligence evaluate cyber resilience for the banking industry.[43]

ii Data breaches

There is currently no mandatory data breach notification requirement in Hong Kong. In October 2015 and then again in January 2019, 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;

40 Sections 24 and 27 of the Telecommunications Ordinance.
41 Sections 59, 60, 85 and 161 of the Crimes Ordinance.
42 Sections 11 and 19 of the Theft Ordinance.
43 www.hkma.gov.hk/media/eng/doc/key-information/speeches/s20190124e1.pdf.

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).

X 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 SMEs 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. The PCPD also reminded the organisations and businesses in Hong Kong to assess the potential impact of the new regulatory framework for data protection in the EU General Data Protection Regulation (GDPR), which became effective on 25 May 2018. The GDPR's extraterritorial effect suggests that the organisations and businesses in Hong Kong that collect and process personal data of EU individuals, should be prepared to comply with the GDPR's requirements.[44] 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.

44 www.pcpd.org.hk/english/data_privacy_law/eu/eu.html.

Chapter 14

HUNGARY

Tamás Gödölle[1]

I OVERVIEW

The introduction of the European General Data Protection Regulation (GDPR) last year 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) is secondary to the general rules that are to be applied throughout the European Union. As of 17 July 2018, the bill for the amendment of the Privacy Act, for the sake of GDPR compliance, was adopted by the Hungarian parliament and was effective as of 25 August 2018

Furthermore, the Hungarian Data Protection Authority (DPA) has been appointed to act as a supervisory authority under the GDPR. 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 order to be compliant with the GDPR, more than 80 sectoral acts were amended by the Hungarian parliament as of 1 April 2019, effective as of 26 April 2019. The omnibus act contained fundamental amendments to the handling of personal data in the field of labour law, security services and activities of private investigators, trade and direct marketing.

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.

1 Tamás Gödölle is a partner at Bogsch & Partners Law Firm.

II THE YEAR IN REVIEW

The year 2019 has mostly been about the preparation for the new regime of the GDPR and also about the application of the GDPR-compliant regulation in the sectoral acts.

As a first-wave preparation aid, the DPA published a localised version[2] of the UK Information Commissioner's Office's 12-point list on how to get ready for the GDPR. To ensure a smooth transition period, the Hungarian government also announced that for a period of one year until May 2019 the SMEs could receive a penalty from the DPA after prior notice was given to them.

As mentioned earlier, in April 2019, an omnibus act was adopted by the Hungarian parliament to make the sectoral acts GDPR-compliant. The omnibus act mostly affected the Hungarian Labour Code, especially the storage of the personal data of employees.

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,[3] 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 Privacy Act as any information relating to a data subject. 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'); the term identifiable natural person was also incorporated in the Privacy Act, which refers to a natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Sensitive data

The former term 'special data' of the Privacy Act was replaced by the term 'sensitive data', which is defined 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

2 Available in Hungarian at: http://naih.hu/felkeszueles-az-adatvedelmi-rendelet-alkalmazasara.html.

3 The text of the Law is available at http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1100112.TV and in English at www.naih.hu/files/Act-CXII-of-2011_EN_23June2016.pdf.

interest organisations, as well as his or her state of health, pathological addictions, sex life or criminal personal data, a definition that was made GDPR-compliant in the same way that the definition of personal data was.[4]

Data controller

The GDPR defined 'controller' as the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; 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. The definition of data controller in the Privacy Act was also made GDPR compliant.

Data processor

The Act identifies a 'data processor' as any natural or legal person or organisation without legal personality that is engaged in processing operations within the framework of and under the conditions set out by law or binding legislation of the European Union, acting on the controller's behalf or following the controller's instructions. 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.

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.[5]

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.[6] 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. The omnibus act of April 2019 brought about significant changes in the field of direct marketing: the regulations in the Act CXIX of 1995 on the Use of Name and Address Information Serving the Purposes of Research and Direct Marketing[7] has changed so that previously collected data of customers can only be used if the legal interest is proved, which can be, for example, the measurement of client satisfaction.

4 ibid., Article 3(3).

5 www.naih.hu/files/AdatvedelmiAuditSzakmaiSzempontokVegleges.pdf.

6 Direct Marketing Act, Section 5.

7 Available in Hungarian at: https://net.jogtar.hu/jogszabaly?docid=99500119.TV

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.

Requirements of preliminary notices

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[8] 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.

For the purposes of preliminary notices Articles 13 and 14 of the GDPR shall also be taken into consideration.

Data security incident register[9]

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.

Additionally, GDPR introduced a new regime for notifying data breaches to the DPA and in certain cases to the data subjects.

8 Available in Hungarian at http://naih.hu/files/tajekoztato-ajanlas-v-2015-10-09.pdf.

9 Implemented in 2015. Applicable from 1 October 2015.

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: the right of access by the data subject, the rights of rectification and erasure (the right to be forgotten), restriction of processing, the 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.[10] 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 or the DPA.[11] 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.

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.[12] 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.

The previously mentioned omnibus act also brought about changes in the field of labour law. The employer is obliged to prove to the employee the necessity, proportionality and the purpose limitation of data handling with prior written notice. Furthermore, the employee shall only present the official documents (e.g., ID card) necessary for the employment

10 Implemented in 2015. Applicable from 1 October 2015.

11 Data Protection Law, Article 17(2).

12 Labour Code, Article 11.

relationship, but the employer is not entitled to make photocopies. The three working days, 30 or 60 days maximum storage periods for camera recordings were also abolished, therefore the employer has the right to set the storage period for the recordings within the framework of GDPR norms such as data minimisation.

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 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)[13] on the risks of public and community cloud services used by financial institutions, namely banks, insurance companies and financial service providers in Hungary.

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).

13 http://felugyelet.mnb.hu/data/cms2364896/vezkorlev_4_2012.pdf.

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 identifies the legal purposes for which health data may be processed.

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.

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 Information Society Services (the e-Commerce Act),[14] 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.[15]

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.[16] The message must contain the email address and other contact details where the individual

14 The e-Commerce Act is available in Hungarian at http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a0100108.tv.

15 e-Commerce Act, Article 14/A.

16 ibid., Article 14(2).

may request the prohibition of the transmission of electronic advertisements.[17] 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 ePrivacy Regulation of the EU that will clarify the rules for direct marketing and consent.

IV INTERNATIONAL DATA TRANSFER

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 GDPR has restructured the requirements concerning data transfers. According to the GDPR data transfers to third countries are allowed in the following cases:

a 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.

b 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.

c 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.

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.

Act I of 2012 on the Labour Code (Labour Code) also lays down the general rules governing workplace privacy.

17 ibid., Article 14(3).

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. 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. 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.

ii 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.

iii Data protection officer

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 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:

a request that an entity cease and desist from infringing the law;
b order the blocking, deletion or destruction of unlawfully processed data;
c prohibit the unlawful processing;
d suspend the transfer of data to foreign countries; and
e impose a fine of up to €20 million.

Under the GDPR and the Privacy 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.

ii Recent enforcement cases

Regarding the higher limit for imposing penalties, the DPA has already issued a penalty of 30 million forints. The penalty was issued to the organisers of Sziget, a well-known Hungarian music festival, and was imposed for the handling of participants' data without any prior

notice or consent and the unnecessarily long period of time of data processing. Furthermore, the participants did not receive any information about their rights if they were not satisfied with the data handling policy of the organisers.

Another significant penalty of 11 million forints was issued by the DPA to a political party (Democratic Coalition) for not reporting a data security incident to the DPA and for not applying a satisfactory level of data security provisions.

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.

Penalties imposed by the DPA are made public via its website.[18] Since the introduction of the new GDPR rules, the upper limits of the fines have seen an significant increase, and so far in the year 2019 the highest penalty imposed was 30 million forints.

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 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 (1) 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 (2) the monitoring of their behaviour as far as their behaviour takes place within the Union.

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

18 www.naih.hu.

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.

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.

Chapter 15

INDIA

Aditi Subramaniam and Sanuj Das[1]

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 had occurred on the subjects of cybersecurity, privacy and data protection until late 2017. In 2013, the 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 unknown reasons, reflecting rather poorly on the government's intention to provide clear, robust and watertight law on these matters.

This is not to say that the urgent need for change in this respect has not been recognised.

Subsequent to the government's launch of a heavily advertised campaign called Digital India in 2015, 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.

In 2016, Parliament passed the Aadhar Act, a piece of legislation aimed at the targeted delivery of financial benefits to the poor. Also under this Act, every Indian citizen was to be issued with a national identity card called the Aadhar card with a unique identification number similar to social security numbers in the United States.

In 2017, the government amended the Income Tax Act 1961 to make it mandatory for taxpayers to link their permanent account numbers to their Aadhar cards in order to file income tax returns, open bank accounts and conduct financial transactions beyond a threshold, to curb tax evasion and money laundering. In essence, this would provide the government with an enormous database of financial information on every citizen of the country, with no real protocols, safeguards or laws to regulate the storage, use and control of

1 Aditi Subramaniam is an associate principal and Sanuj Das is a managing associate at Subramaniam & Associates.

this information. The Department of Telecommunications also sought to use Aadhar cards as tools for subscriber verification from existing mobile telephone subscribers and made it mandatory for these cards to be linked to new mobile telephone connections.

The Aadhar Act was challenged in a series of petitions that questioned its constitutional validity. One 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 by a nine-judge constitutional bench of the Supreme Court, which held privacy to be a fundamental right of every citizen under the Constitution. The move to link Aadhar cards to the financial and biometric information of all Indian citizens was also challenged before the Supreme Court. In September 2018, the Supreme Court upheld the Aadhar Act but struck down certain provisions therein. The Court stated that while the use of Aadhar cards will remain mandatory for the filing of income tax returns and issuance of permanent account numbers, Aadhar cards would no longer need to be linked to individual bank accounts or mobile telephone connections. Along with the recognition of privacy as a constitutionally guaranteed fundamental right by the Supreme Court in 2017, this development indicated the genuine interest of the judiciary in compensating for years of legislative apathy with specific regard to data protection and privacy.

II THE YEAR IN REVIEW

The government empanelled a 10-member committee under the chairmanship of Justice BN Srikrishna, a retired Supreme Court judge, to put together detailed reviews of current data protection laws as well as suggestions on how to fill judicial and legislative lacunae. The committee compiled an extensive report containing a draft data protection framework, along with the draft Personal Data Protection Bill 2018. Since 2011, various iterations of the Privacy Bill have been released, the latest of which was the Data Privacy Bill 2017. It appears that the draft Personal Data Protection Bill 2018 may be intended to replace the Data Privacy Bill 2017, although the intention of the legislature in this regard is unclear at the moment. Barring some limited overlap, both documents cover different aspects of the law, and perhaps the public interest will be better served if both were to coexist. A number of rounds of consultation have already been conducted on the draft Personal Data Protection Bill 2018, and extensive feedback has been submitted by various stakeholders, including the US government. The draft Personal Data Protection Bill 2018 may be brought before in Parliament later this year.

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[2]

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,[3] which require entities holding users' sensitive personal information to maintain certain specified security standards;

b the Information Technology (Intermediaries Guidelines) Rules,[4] which prohibit content of a specific nature on the internet, and an intermediary, such as a website host, is required to block such content;

c the Information Technology (Guidelines for Cyber Cafe) Rules,[5] which require cybercafés 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,[6] 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.

2 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.

3 meity.gov.in/sites/upload_files/dit/files/GSR313E_10511(1).pdf.

4 meity.gov.in/sites/upload_files/dit/files/GSR314E_10511(1).pdf.

5 meity.gov.in/sites/upload_files/dit/files/GSR315E_10511(1).pdf.

6 meity.gov.in/sites/upload_files/dit/files/GSR316E_10511(1).pdf.

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. Additionally, the draft Personal Data Protection Bill 2018, referred to above, may also be introduced into law later this year.

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:

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.[7]

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.[8]

7 www.cert-in.org.in.

8 catindia.gov.in/Default.aspx.

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:

a passwords;
b financial information, such as bank account, credit card, debit card or other payment instrument details;
c physical, physiological and mental health conditions;
d sexual orientation;
e medical records and history;
f biometric information;
g any details relating to the above clauses as provided to a body corporate for the provision of services; or
h 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.

The 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'.

The draft Personal Data Protection Bill 2018, defines 'sensitive personal data' as personal data revealing, related to or constituting passwords; financial data; health data; official identifier; sex life; sexual orientation; biometric data; genetic data; transgender status; intersex status; caste or tribe; religious or political belief or affiliation; or any other category of data specified by the Authority under Section 22 where the Authority is the data protection authority envisaged by the bill, and Section 22 empowers this authority to specify further categories of sensitive personal data as it deems necessary to do so. The draft Personal Data Protection Bill 2018 also defines 'personal data' as 'data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, or any combination of such features, or any combination of such features with any other information.' Unlike the IT Act and Rules, the draft Personal Data Protection Bill 2018 also contains definitions for 'processing', 'data fiduciary', 'data processor', 'data principal' and, crucially, 'consent'.

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. The draft Personal Data Protection Bill 2018 defines 'consent' and 'explicit consent' and provides grounds, including the functions of the state, or compliance with a court order, for the lawful processing of personal data as well as sensitive personal data.

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. The draft Personal Data Protection Bill 2018 prescribes that personal data be processed only for 'clear, specific and lawful' purposes and for such purposes that the data principal would 'reasonably expect the personal data to be used for, having regard to the specified purposes', as well as the 'context and circumstances' (Section 5). It also limits the collection of personal data in Section 6 to such data that is necessary for the purposes of processing.

Data retention

Section 67C of the IT Act requires that an intermediary preserve and retain information in a manner and format and for such period of time as prescribed by the central government. The draft Personal Data Protection Bill 2018 states that retention by fiduciaries may occur only for so long as it is 'reasonably necessary to satisfy the purpose for which it is processed' (Section 10). The draft Personal Data Protection Bill 2018 also allows for longer periods of retention if required by compliance with legal obligations, and prescribes periodic reviews by data fiduciaries for an ongoing assessment of the continued necessity of the retention of personal data. The data protection authority envisaged by the draft Personal Data Protection Bill 2018 must also, under Section 61, develop a code of practice for 'measures pertaining to the retention of personal data under section 10'.

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. The draft Personal Data Protection Bill 2018 requires in Section 38 that based on certain criteria, the data protection authority envisaged by the bill shall notify certain data fiduciaries as being 'significant'. Significant data fiduciaries will be required to register with the authority in a manner specified by it, and will also be subject to data protection impact assessments, data audits, etc. Under Section 38, the data protection authority may also require registration by other data fiduciaries at its discretion, even if such entities are not 'significant'.

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. Sections 24 of the draft Personal Data Protection Bill 2018, teases out this right in more detail, providing for the data principal to obtain from the data fiduciary in a clear and concise manner, confirmation on whether its personal data is being (or has been) processed and a brief summary of processing activities. Section 28 states the procedure by which such rights may be exercised by the data principal.

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. The draft Personal Data Protection Bill 2018 provides for a separate, detailed right to rectification of errors, such as inaccurate or misleading personal data, incomplete personal data, and outdated personal data, in Section 25, and a right to be forgotten in Section 27. Incidentally, Section 27 provides for the data principal's right to restrict or prevent continuing disclosure of personal data by the data fiduciary, but only if the data protection authority, through an adjudicating officer, determines that any of the listed grounds for restriction or prevention of disclosure have been found. Further, there is no reference in Section 27 to the deletion of data already in possession of the data fiduciary.

The Supreme Court of India in a nine-judge bench decision in August 2017 in *KS Puttaswamy & Ors v. Union of India & Ors*[9] 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. As mentioned above, Section 27 of the draft Personal Data Protection

9 http://supremecourtofindia.nic.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf.

Bill 2018 provides for a data principal's right to restrict or prevent continuing disclosure of personal data by the data fiduciary, but only if the data protection authority, through an adjudicating officer, determines that any of the listed grounds for restriction or prevention of disclosure have been found.

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. The draft Data Protection Bill, 2018, in Section 28, allows for a data principal to complain to the data protection authority if it is unreasonably hindered by the data fiduciary in the exercise of its rights.

iii Specific regulatory areas

Financial privacy

Public Financial Institutions (Obligation as to Fidelity and Secrecy) Act 1983[10]

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[11]

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[12]

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[13]

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.

10 http://lawmin.nic.in/ld/P-ACT/1983/The%20Public%20Financial%20Institutions%20(Obligation%20as%20to%20Fidelity%20and%20Secrecy)%20Act,%201983.pdf.

11 http://fiuindia.gov.in/pmla2002.htm.

12 www.cibil.com/sites/default/files/pdf/cicra-act-2005.pdf.

13 https://rbidocs.rbi.org.in/rdocs/Publications/PDFs/86706.pdf.

Foreign Contribution Regulation Act 2010[14]

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

Under the Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations 2002 (Code of Ethics Regulations 2002)[15] 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.

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.

14 https://fcraonline.nic.in/home/PDF_Doc/FC-RegulationAct-2010-C.pdf.

15 http://niti.gov.in/writereaddata/files/1.pdf.

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 per the draft Personal Data Protection Bill 2018, cross-border data transfers outward from India may be regulated by the central government. Section 40 lists that every data fiduciary shall ensure the storage of at least one serving copy of personal data on a server or data centre located in India, and the central government shall notify categories of personal data as being critical personal data, to be processed only in a server or data centre in India. In Section 41, sub-section 2, the draft Personal Data Protection Bill 2018 states that the central government will be entitled to permit such transfers only under certain specific circumstances.

As worded, Section 7 of the IT Rules 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.*
> 2. *The international standard IS/ISO/IEC 27001 on 'Information Technology – Security Techniques – Information Security Management System – Requirements' is one such standard referred to in sub-rule (1).*
> 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. Similarly, the draft Personal Data Protection Bill 2018 also envisages the establishment of a data protection authority, which may require registration by data fiduciaries under certain circumstances, as described above in Section III.ii.

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 Bills and the draft Data Protection Bill, 2018, conceptualise the creation of a data protection authority for the enforcement of data protection legislation and to oversee compliance with it. These Bills will likely become the principal data protection legislation if enacted, and in that event, 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 or the draft Data Protection Bill, 2018, 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

Karmanya Singh Sareen & Anr v. UOI & Ors[16]

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

16 (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.

KS Puttaswamy & Ors v. Union of India & Ors[17]

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 issued 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

17 http://supremecourtofindia.nic.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf.

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.[18]

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.

18 www.cnbc.com/2018/07/11/cambridge-analytica-must-answer-india-says-minister-prasad.html.

Chapter 16

JAPAN

Tomoki Ishiara[1]

I OVERVIEW

In Japan, the Act on the Protection of Personal Information[2] (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[3] 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,[4] the Japan Financial Services Agency,[5] and the Ministry of Economy, Trade and Industry.[6] Under the amended IPPI, however, the guidelines (the APPI Guidelines)[7] 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.[8]

1 Tomoki Ishiara is counsel at Sidley Austin Nishikawa Foreign Law Joint Enterprise.

2 Act No. 57 of 30 May 2003, enacted on 30 May 2003 except for Chapters 4 to 6 and Articles 2 to 6 of the Supplementary Provisions; completely enacted on 1 April 2005 and amended by Act No. 49 of 2009 and Act No. 65 of 2015: www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf.

3 Article 2 of the Order for Enforcement of the Act on the Protection of Personal Information (Cabinet Order 506, 2003, enacted on 10 December 2003).

4 The Guidelines on Protection of Personal Information in the Employment Management (Announcement No. 357 of 14 May 2012 by the Ministry of Health, Labour and Welfare).

5 The Guidelines Targeting Financial Sector Pertaining to the Act on the Protection of Personal Information (Announcement No. 63 of 20 November 2009 by the Financial Services Agency).

6 The Guidelines Targeting Medical and Nursing-Care Sectors Pertaining to the Act on the Protection of Personal Information (Announcement in April 2017 by the PCC and the Ministry of Health, Labour and Welfare).

7 The General Guidelines regarding the Act on the Protection of Personal Information dated November 2017 (partially amended March 2017).

8 The Guidelines Targeting Financial Sector Pertaining to the Act on the Protection of Personal Information (Announcement in February 2017 by the PCC and the Financial Services Agency).

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 government[9] 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[11]

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 Act[12] 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.

10 http://japan.kantei.go.jp/policy/it/20140715_2.pdf.

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:

a no consent is necessary in accordance with the following exceptions to Article 23(1):
- cases based on laws and regulations;
- 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;
- 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
- 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,[15] and when there is a possibility that obtaining a principal's consent would interfere with the execution of these duties;

b 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

c 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.

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.[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.

14 Article 24 APPI.

15 Article 23 APPI.

16 Article 36(1) APPI.

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 past record as 'special-care-required personal information' (sensitive personal information), along with any other information that may be the focus of social discrimination.[17] 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.[18]

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.[19] 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;[20]

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;[21] and

c establishes criminal liability for providing or stealing personal information with a view to making illegal profits.[22]

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,[23] 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

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).

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 amended APPI. This authority consists of one chair and eight commission members.[24] 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[25] and the Act on Specified Commercial Transactions,[26] 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.

a Information on trade union membership or an individual's sexual orientation[27] shall be regarded as sensitive information in Japan as well as in the EU.

b Personal data that will be deleted within six months[28] shall be protected as personal data.

c The purpose of use of personal information provided by a third party is limited to that originally set by the third party.

d 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 For the anonymisation of personal information coming from the EU, the complete deletion of a method of re-identification would be required.[29]

24 www.ppc.go.jp/en/aboutus/commission/.

25 Act No. 26 of 17 April 2002.

26 Act No. 57 of 4 June 1976.

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.

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:

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:

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.

a state organs;
b local governments;
c incorporated administrative agencies, etc.;[36] and
d local incorporated administrative institutions.[37]

Personal data[38]

'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)[39] 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.[40] Furthermore, the JFSA Guidelines prohibit the collection, use or provision to a third party of sensitive information,[41] 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

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).
38 Article 2(6) APPI.
39 The Guidelines Targeting Financial Sector Pertaining to the Act on the Protection of Personal Information (Announcement No. 63 of 20 November 2009 by the Financial Services Agency).
40 Article 6(1) of the JFSA Guidelines.
41 Article 6(1)1–8 of the JFSA Guidelines.

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. 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'.[42]

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.[43]

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.[44]

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.[45]

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,[46] 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.[47]

42 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.

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.[48]

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.[49]

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

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.

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.

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 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

54 Article 23(5)(iii) APPI.

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.

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 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

b 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. Since 23 January 2019, the EU has been considered a jurisdiction that provides the same level of protection of personal data in Japan. The PPC will review this designation within two years and then continues to review every four years or at any time when the PPC considers it to be necessary.[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.

57 Article 75 APPI.

58 Article 23(1) APPI.

59 Article 24 APPI.

60 Article 11 Rules of the PPC.

61 The PPC Announcement No. 1 (23 January 2019), the designated countries include Iceland, Ireland, Italy, the United Kingdom, Estonia, Austria, the Netherlands, Cyprus, Greek, Croatia, Sweden, Spain, Slovakia, Slovenia, Czech Republic, Denmark, Germany, Norway, Hungary, Finland, France, Bulgaria, Belgium, Poland, Portugal, Malta, Latvia, Lithuania, Liechtenstein, Romania and Luxembourg.

62 Article 20 APPI.

Systemic security control measures[63]

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 measures[64]

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.

Physical security control measures[65]

a Implementing controls on entering and leaving a building or room where appropriate;
b preventing theft, etc.; and
c physically protecting equipment and devices.

Technical security control measures[66]

a Identification and authentication for access to personal data;
b control of access to personal data;
c management of the authority to access personal data;
d recording access to personal data;
e countermeasures preventing unauthorised software on an information system handling personal data;
f measures when transferring and transmitting personal data;
g measures when confirming the operation of information systems handling personal data; and
h monitoring information systems that handle personal data.

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.
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.

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.[67] However, in the following circumstances, the business operator may keep all or part of the retained personal data undisclosed where disclosure:

a is likely to harm the life, person, property, or other rights or interests of the person or a third party;

b is likely to seriously impede the proper execution of the business of the business operator handling the personal information; or

c violates other laws and regulations.[68]

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]

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.

69 Article 44 APPI.

Main penalties[70]

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 report[72] 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 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[75] 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

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.

75 3-3-2 of the APPI Guidelines, p. 41.

76 www.soumu.go.jp/menu_news/s-news/01kiban05_02000017.html (available only in Japanese).

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 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.

Further, in a case where a different plaintiff filed a lawsuit against Benesse Corporation, on 20 June 2018, the Tokyo District Court denied measurable damages caused by Benesse Corporation's negligence as in the Osaka High Court decision above. The plaintiff appealed and on 27 June 2019, the Tokyo High Court overturned the District Court's decision, holding that the appellant (plaintiff) was mentally injured by any possibility of the use of his personal information without his consent (e.g., unknown persons could contact him directly by using his leaked private address) and the compensation for such mental damage amounts to ¥2,000 per data subject.

77 Announcement No. 695 of 31 August 2004 by the MIC.

78 www.soumu.go.jp/menu_news/s-news/01kiban08_02000094.html (available only in Japanese).

79 Nikkei News website article on November 6 of 2012 (available only in Japanese): www.nikkei.com/article/DGXNASFD05015_V01C12A1CN8000.

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,[80] 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[81] (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,[82] 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.[83]

Finally, the Basic Act on Cybersecurity, which provides the fundamental framework of cybersecurity policy in Japan, was passed in 2014.[84]

80 Act No. 45 of 1907, Amendment: Act No. 74 of 2011.

81 Act No. 128 of 199, Amendment: Act No. 12 of 2012.

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).

83 See NISC, 'Japanese Government's Efforts to Address Information Security Issues: Focusing on the Cabinet Secretariat's Efforts': www.nisc.go.jp/eng/pdf/overview_eng.pdf; and the government's international cybersecurity strategy: www.nisc.go.jp/active/kihon/pdf/InternationalStrategyonCybersecurityCooperation_e.pdf.

84 Act No. 104 of 12 November 2014.

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]

a internal report on the data breach, etc. and measures to prevent expansion of the damage;

b investigation into any cause of the data breach, etc.;

c confirmation of the scope of those affected by the data breach, etc.;

d consideration and implementation of preventive measures;

e notifications to any person (to whom the personal information belongs) affected by the data breach etc.;

f prompt public announcement of the facts of the data breach, etc. and preventive measures to be taken; and

g 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. In this respect, the PPC has continued to hear from relevant parties for its review of the APPI every three years. In particular, on 25 April 2019, the PPC published an intermediate summary of discussion points for review every three years. The topics include, but are not limited to, the data portability, clarification of standard of report to agency. Also, the PPC has recently published a study report on how the personal data has been effectively collected and used under the APPI. It is expected that the PPC may propose some revisions of the APPI based upon the above activities and achievements.

85 PPC Announcement No.1 of 2017.

86 Articles 40–42 APPI.

ii The judicial reaction to the leaking of personal information in Japan

As stated in Section VII, Tokyo High Court expressed its views regarding the damage caused by a data breach case in the *Benesse* case and this case has been appealed to the Supreme Court. In addition, another case (see Section VII.ii) in connection with Benesse's data leakage is still pending before Osaka High Court. The Supreme Court may revisit the *Benesse* data leakage case and clarify the extent and scope of the duty of care of business operators handling personal information and the calculation of damages arising from data breaches caused by a violation of such duty of care.

Chapter 17

MALAYSIA

Shanthi Kandiah[1]

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.

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 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 Minister of Communications and Multimedia (Mr Gobind Singh Deo) announced that the PDPA is currently being reviewed by the Ministry of Communications and Multimedia to streamline international requirements on personal data protection including key takeaways of the European Union's General Data Protection Regulation (GDPR).[4]

To date, the Commission's enforcement actions tend towards enforcement of straightforward breaches such as offences for processing personal data without a certificate of registration. As at July 2019, there are at least five enforcement cases that have resulted in conviction by the court. A majority of the convictions are for the offence of processing personal data without a certificate of registration.[5]

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:

a personal data collection forms and privacy notice;

b internal standard operating procedures for personal data management within the organisation;

4 Mr Gobind Singh Deo, from 'Gobind: Personal data protection law to be updated soon' dated 18 March 2019, New Straits Times (https://www.nst.com.my/news/government-public-policy/2019/03/470358/gobind-personal-data-protection-law-be-updated-soon)

5 Section 16(4) of the PDPA.

c person in charge of personal data management within the organisation and his or her awareness of the legal requirements; and
d compliance with the seven data protection principles in the PDPA.

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 (NACSA), 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:

a utilities sector (electricity);[8]
b insurance/*takaful* industry;[9]
c banking and financial sector;[10]
d licensees under the Communications and Multimedia Act 1998;[11] and
e the Malaysian aviation sector.[12]

A code of practice for legal practitioners is also expected to be introduced.

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.[13]

6 See Section IX.i.
7 Section 5(2) of the PDPA.
9 With effect from 23 December 2016.
10 With effect from 19 January 2017.
11 With effect from 23 November 2017.
12 With effect from 21 November 2017.

Personal data

Three conditions must be fulfilled for any data to be considered as 'personal data' within the ambit of the PDPA.[14]

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.[15] 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.[16]

Sensitive personal data

Sensitive personal data is defined as any personal data consisting of information as to:

a the physical or mental health or condition of a data subject;

b his or her political opinions;

c his or her religious beliefs or other beliefs of a similar nature;

d the commission or alleged commission by him or her of any offence; or

e any other personal data as the minister responsible for personal data protection (currently the Minister of Communications and Multimedia) may determine.[17]

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.[18]

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 that 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. There appears to be some doubt about the application of the PDPA to social media companies

14 Section 2 of the PDPA.

15 Section 2 of the PDPA.

16 See also Section 45(2)(c) of the PDPA.

17 Section 2 of the PDPA.

18 Section 40(1) of the PDPA.

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.[19]

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, retail and wholesale); and
k transportation.

The list of data users was expanded in 2016 to include two additional sectors: pawnbroking and money lending.[20] Failure to register by these categories of data users is an offence.[21]

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 or 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.[22]

19 Section 2(2) of the PDPA.

20 Personal Data Protection (Class of Data Users) (Amendment) Order 2016, which came into effect on 16 December 2016.

21 Section 16(4) of the PDPA.

22 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.[23]

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

23 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.

iii Data subjects' rights

A data subject has various rights to his or her personal data kept by data users. These are:

a the right of access to personal data;[24]
b the right to correct personal data;[25]
c the right to withdraw consent;[26]
d the right to prevent processing likely to cause damage or distress;[27] and
e the right to prevent processing for purposes of direct marketing.[28]

Complaint

Under the PDPA, the data subject can make a written complaint to the Commissioner about an act, practice or request:

a specified in the complaint;
b engaged in by the data user specified in the complaint;
c that relates to personal data of which the individual is the data subject; and
d that may be in contravention of the PDPA including any codes of practice.[29]

Upon receiving a complaint, the Commissioner may choose to conduct an investigation in relation to the relevant data user to ascertain whether the act, practice or request specified in the complaint contravenes the PDPA.[30] In the event that the complainant withdraws the complaint, the Commissioner may carry out or continue an investigation where the Commissioner is of the opinion that it is in the public interest to do so.[31] The enforcement powers of the Commissioner are further discussed in Section VII below.

iv 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

24 Section 30 of the PDPA.
25 Section 34 of the PDPA.
26 Section 38 of the PDPA.
27 Section 42 of the PDPA.
28 Section 43 of the PDPA.
29 Section 104 of the PDPA.
30 Section 105(1) of the PDPA.
31 Section 107 of the PDPA.

Innovation has unveiled the National Internet of Things Strategic Roadmap (the Roadmap) where a centralised regulatory and certification body will be established to address privacy, security, quality and standardisation concerns.

v 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.

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.[32] 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.[33]

The Guidelines on Data Management and MIS[34] 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.[35]

32 Schedule 11 of the FSA sets out a list of permitted disclosures.

33 See also Section 165 of the Islamic Financial Services Act 2013.

34 Management Information System.

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[36] 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 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 July 2019, 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.

36 (PCP) No. 1/2017.

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 Data subject opt-in, opt-out, access, deletion and portability rights

In addition to the need for consent, the Public Consultation Paper (No. 1/2014) titled the Guide to Dealing with Direct Marketing under the Personal Data Protection Act (PDPA) 2010 provides that an individual must be given the right to refuse the use of personal data for direct marketing. In the case of direct marketing by electronic means, an opt-out right must be made available on every subsequent marketing message. The right of portability is not available under the PDPA.

v 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 on their behalf, but this is not currently mandated.

vi 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.[37] 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.

37 The Personal Data Protection Standards 2015.

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.

vii 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 (MCMC) 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.

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:

a conducting inspections on data users' personal data systems;
b publishing reports that set out any recommendations arising from the inspections; and
c 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:

a conducting investigations on the commission of any offence under the PDPA;
b conducting searches and seizure of data users' computerised data, documents, equipment, systems and properties, with or without a warrant;
c requiring the production of computers, books, accounts, computerised data or other documents kept by data users; and
d 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.[38]

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.[39]

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.

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 – MyCERT Incident Statistics – indicate that in 2018 there were a total of 10,699 reports on cyber-related incidents.[40] Statistics from January to May 2019 indicate that there have been over 3,743 reports on cyber-related incidents.[41] 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. However, in August 2018, a Public Consultation Paper (No. 1/2018) titled the Implementation of Data Breach Notification (the DBN Consultation Paper) was issued. The DBN Consultation Paper suggests that data users are required to, among other things, notify the Commissioner within 72 hours of becoming aware of the data breach, provide details of the data breach, provide details on actions taken to contain the breach and whether the organisation's staff has received training on data protection in the last 24 months.

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

38 Section 133(1) of the PDPA.

39 http://www.pdp.gov.my/index.php/my/pusat-media/berita/989-pengguna-data-yang-telah-dikenakan-tindakan-di-bawah-akta-perlindungan-data-peribadi-2010-akta-709.

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 CNIIs 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.

On 18 July 2019, the BNM issued the policy document on Risk Management in Technology (RMiT policy document) that sets out its requirements with regard to financial institutions' technology risk management framework and practices proportionate to the size and complexity of the financial institutions. The RMiT policy document sets out the board and senior management responsibilities, the responsibilities of the chief information security officer, the requirement for financial institutions to establish a robust framework for managing technology projects, the requirement to conduct due diligence on third-party service providers, the requirement to conduct risk assessment prior to conducting cloud services, and to provide adequate and regular technology and cybersecurity awareness training.

The Securities Commission Malaysia has also issued its Guidelines on Management of Cyber Risk,[42] which sets out a framework to address cybersecurity resilience for capital market participants' management of cybersecurity risks.

i Cyber laws

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.

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;[43]

b the offence of using an apparatus or device without authority;[44]

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;[45]

d the offence of interception and disclosure of communications;[46] and

e the offence of damage to network facilities.[47]

42 With effect from 31 October 2016.

43 Section 233(1)(a) of the CMA.

44 Section 231 of the CMA.

45 Section 233 of the CMA.

46 Section 234 of the CMA.

47 Section 235 of the CMA.

Other cyberoffences include:

a cyberpornography and exploitation of children;[48]
b online sedition and internet defamation;[49]
c misuse of computers;[50]
d prostitution and other illegal cybersexual activities; and
e cyberterrorism.[51]

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 114A, 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 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 Minister of the MCMC 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 among data users on their data protection obligations.

Recent incidents such as the MOMO challenge hoax, ransomware, banking account leaks and other data breaches were reported and received wide media coverage in Malaysia. The Chief Executive Officer of Cybersecurity Malaysia stated that cybersecurity is currently perceived as a cost rather than an investment for businesses. He further stated that with the increased use of technology, cybersecurity should be a default feature in all businesses

48 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.

49 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.

50 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.

51 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).

regardless of their size and not an afterthought.[52] It is understood that the Personal Data Protection Commission is still seeing low levels of awareness in relation to the PDPA, particularly among smaller enterprises. We expect to see more businesses improving their data protection framework and measures to safeguard the interests of the data subjects as well as their own.

In light of the GDPR, the Minister stated that while there is no timeframe for the review of the PDPA, the review exercise is still ongoing and it is hoped that a new framework will be formulated or that a proposed amendment will be brought to Parliament. The release of the DBN Consultation Paper is expected to be implemented by imposing conditions on the certificate of registration issued to the data users by the Commissioner. As such, this applies to the 13 classes of data users as specified in Section III.ii above. 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). 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.

52 Datuk Dr Amiruddin Abdul Wahab, from 'Cybersecurity should be the default feature in all businesses' dated 12 May 2019, *New Straits Times* (https://www.nst.com.my/business/2019/05/487760/cybersecurity-should-be-default-feature-all-businesses).

Chapter 18

MEXICO

César G Cruz Ayala, Diego Acosta Chin and Marcela Flores González[1]

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 into an individual's person, family, domicile, documents or belongings (including any wiretapping 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, disclosing 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

1 César G Cruz Ayala is a partner, and Diego Acosta Chin and Marcela Flores González are associates at Santamarina y Steta, SC.

move, the former IFAI amended its internal regulations so that it could assume the necessary 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 2019, the INAI continued to enforce the Private Data Protection Law and, at the same time issued opinions and guidelines that may in the future translate into amendments to the Private Data Protection Law, particularly with respect to the use of mobile devices.

On 28 September 2018 the Federal Official Gazette published the decree issuing 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).

On 24 November 2018 INAI published a bulletin informing the public that it would verify if the Attorney General of the Republic (FGR) breached the Governmental Data Protection Law by using Pegasus, software for criminal investigations that was allegedly used to spy on journalists, activists and human rights observers. The bulletin detailed how the current FGR had to demonstrate that the software had been uninstalled from the equipment of the Unit for Cyber Investigations and Technological Operations of the Criminal Investigation Agency, as well as from any other equipment and submit evidence on the politicies, methods and techniques followed to uninstall such software.

On 4 January 2018 Congressman Ramón Villagómez Guerrero submitted a bill to modify the Private Data Protection Law, to standardise it with the Governmental Data Protection Law, and include a definition of concepts that are currently defined in the Regulation; this bill has not yet been approved by Congress.

On 8 February 2019, the INAI made available to data controllers a tool called the 'data breach evaluator', which allows data controllers to register and record the current security measures within companies with the purpose of minimising the occurrence and impact of data breaches. This tool was created exclusively to help data controllers improve their security measures. It is our understanding that the INAI does not have access to the information registered in this tool.

On 25 February 2019, the INAI published a bulletin stating that as a result of a data breach in which the National Savings and Financial Services Bank (Bansefi) exposed the personal data of a user (including their name, address, bank account information and email address) on their website from 2013 to 2018, the Internal Control Body of Bansefi should impose penalties on the officer responsible for disclosing the personal data. The penalty may not be paid with public resources.

On 21 and 22 March 2019, the Ministry of Finance and Public Credit issued several provisions that amend, add and eliminate different articles of the General Provisions for the Prevention of Money Laundering and Terrorism Financing applicable to the services that may be rendered by financial entities such as credit institutions and exchange offices. These are services such as opening accounts, entering into agreements or performing financial operations through the use of the internet or mobile devices. Financial entities will request geolocalisation of clients, as well as biometric data such as voice and image matching to perform such operations, and will, therefore, require express written consent from clients.

In May 2019, the INAI published non-binding guidelines in relation to different tools and applications that may be used by parents to supervise or limit access and content in mobile devices used by their children. This is to protect children from disclosing their personal data on unsecured sites.

On 4 July 2019, the INAI published a bulletin stating that it will initiate a constitutional proceeding before the Mexican Supreme Court against the Administrative Liability Law for the state of Nuevo Leon issued on 7 June 2019, arguing that several provisions included violate the data protection right provided in the Constitution, specifically, the principles of legality, purpose and proportionality established in the Governmental Data Protection Law.

On 16 July 2019, the INAI published certain recommendations to prevent theft, disclosure or alteration of personal data in this digital era, including security configurations, mobile applications, and software that are considered useful so that users can safely protect and maintain their privacy and personal data while using the internet.

The Organization of American States (OAS) published a study on the state of cybersecurity in the Mexican financial system to increase awareness of the growing threats to digital security in the Latin American and Caribbean region.

In a recent interview with local newspapers, the Commissioner-President of the INAI said that considering recent data breaches it is important to amend the Private Data Protection Law to stipulate that data controllers should have the obligation to inform the INAI of any data breaches that they suffered. However, no bill to amend the Private Data Protection Law has been submitted yet.

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 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 forth 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 Ministry 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, which were also issued by the Ministry 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 record it 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 disclosure or distribution;
- 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 Private Data Protection Law is based on the principles by which each data controller must abide to protect the personal data being processed. These principles are summarised as follows.

a Legality: all personal data shall be lawfully collected and processed.

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 is 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. Regarding sensitive personal data, reasonable efforts shall be made to keep the period of processing to a minimum.

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.

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. Its collection shall not be made through fraudulent or deceitful means.

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. Currently, many proceedings to verify compliance have resulted from claims filed by data subjects; however, the INAI determined to initiate *ex officio* proceedings when 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:

a full: a full privacy notice must be used when the personal data is personally collected from a data subject, and must include all elements contained in the corresponding provisions of the Private Data Protection Law, the Regulations and the Guidelines;

b simplified: a simplified privacy notice may be used when the personal data is 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

c 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 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.

The data controller shall describe the means available to the data subject to exercise their right to access, rectify, cancel or oppose the processing of their personal data (ARCO rights), as well as to withdraw consent (withdrawal), either in whole or in part, with respect to the processing of personal data, and to limit the use or disclosure of personal data (data limitation), collectively with the ARCO rights and the right of withdrawal (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, awareness in Mexico regarding the protection of personal data is still a major challenge, considering the lack of knowledge (and, in some cases, interest) together with the degree of specialisation of this matter, which 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 Data subject rights

Data subjects have the following rights, which are intended 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 required 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, either in whole or in part, with respect to the processing of personal data, and may limit the use or divulgement of personal data collectively with the ARCO rights and the right of withdrawal. Additionally, a data subject has the right to opt out or join lists of those unwilling to receive marketing communications or materials kept by the data controller, Profeco or Condusef.

In addition, data subjects have the right to file claims before the INAI if that data controller fails to address a claim concerning the data subject's ARCO rights or when the resolution of the data controller does not satisfy the data subject. If, as a result of that claim, the INAI becomes aware of a breach of the Private Data Protection Law, it may impose penalties on a data controller. However, the Private Data Protection Law makes no provision for remedies or financial recovery for the data subject as a result of a breach of its data protection rights. Notwithstanding this, data subjects have the right to file a claim before civil courts to seek indemnification resulting from moral damage.

iv 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).

v 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;

d 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;

e necessary or legally required to protect the public interest or the prosecution or enforcement of justice;

f required for the acknowledgment, exercise or defence of a right in a judicial proceeding; or

g 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 is 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.

Data controllers have the obligation to include in their privacy notice a mechanism for data subjects to exercise their ARCO rights or withdraw consent, either in whole or in part, with respect to the processing of personal data, and to limit the use or disclosure of personal data. Additionally, data controllers should make opt-out mechanisms or lists for those unwilling to receive marketing communications available to data subjects. These lists are kept by the data controller, Profeco or Condusef.

In terms of the Private Data Protection Law, while processing personal data, a data controller must distinguish such processing based on the following: (a) those purposes that, based a contractual relationship between data controller and data subject, require the processing of personal data, in which case consent for such processing is not required and the opt-out option would not be available; and (b) those secondary purposes where compliance with any commitments is not required under any relationship between the data controller and data subject, in which case the data subject is entitled to opt out and the data controller must provide mechanisms allowing the data subject to opt out prior to such processing.

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 alleged 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 an alleged breach of the Private Data Protection Law, a proceeding to impose penalties will commence assessing the infringement. The available penalties include the following:

a 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;

b fines representing an amount of between 100 and 320,000 times the UMA,[2] which is published by the National Institute of Statistics and Geography, which will be determined based on the nature of the infringement; and

c 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 items (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 damages 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:

2 Between 8,449 and 27,036,800 Mexican pesos in 2019.

a the nature of the personal data;
b the inappropriateness of the failure to comply with the claim of the data subject;
c whether the action or omission was deliberate;
d the economic capacity of the data controller; and
e 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.[3]

In recent years, the INAI has fined, inter alia, financial institutions, telecom companies and healthcare providers. However, most of these fines have been challenged by the data controllers concerned and the proceedings are pending resolution.

Since the enactment of the Private Data Protection Law, the INAI has been actively advertising the importance of complying with this law and pursuing those cases in which there are important breaches and it has imposed fines on several companies to create awareness of the importance of complying with the law. The following are relevant cases in recent years that are worth mentioning.

Hospital

A fine of 4.6 million Mexican pesos was imposed on 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.

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.

ii Recent enforcement cases

Considering that many of the resolutions issued by the INAI have been challenged by the data controllers and are pending resolution, most cases shown on the INAI's webpage for 2018 have been removed from the webpage, or the name of the parties involved have been erased. However, this year many of the proceedings initiated before the INAI involve cases against governmental entities or requests for the disclosure of public information.

3 168,980 Mexican pesos in 2019.

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 to 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

c 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 to the Private Data Protection Law.

iii Private litigation

The Private Data Protection Law makes no provisions 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 consider 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.

The Private Data Protection Law does not impose any obligation against data controller on the location in which personal data should be stored or kept or even if whether such should remain in Mexico. As described in Section IV, under the Private Data Protection Law, an international communication of personal data originating from a data controller may be either a 'transfer' or a 'remittance'. It is important to note that any international data transfer will be subject to consent of the data subject and 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 and detailed in the corresponding privacy notice.

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;

c 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

d 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.

Although this is a non-binding document, in an attempt to avoid further cyberattacks or threats, the Cybersecurity Study includes cybersecurity recommendations for the financial system in Mexico including:

a preparedness and governance: having one responsible body or corporate governance body to lead information security and fraud prevention using digital means;

b detection and analysis of digital security events: prioritising the development of capacities using emerging digital technologies, such as Big Data, artificial intelligence and related technologies;

c digital security incident management, response, recovery and reporting: investigating the source of an incident and guaranteeing the design and implementation of polices or processes for its containment, response and recovery;

d training and awareness: providing training plans and carrying out prevention campaigns; and

e financial system authorities and regulatory bodies: issuing guidelines, recommendations and instructions on digital security best practices and verifying the provision of reporting mechanisms.

X 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.

Although the General Data Protection Regulations (GDPR) applicable in the European Union (EU) are not enforceable per se in Mexico, some provisions of the GDPR are intended to address processing beyond the borders of the EU, to the extent that it is with respect to the personal data of EU citizens or residents of EU Member States. As a result, it is foreseeable that those entities that intend to carry out 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 that process personal data on behalf of EU companies or subsidiaries, may be asked to meet with these new standards imposed by the GDPR.

Chapter 19

POLAND

Anna Kobylańska, Marcin Lewoszewski, Aleksandra Czarnecka and Karolina Gałęzowska[1]

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). As a result, on 4 May 2019 the Derogation Act,[2] which introduced changes to almost 170 Polish acts, entered into force. 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.[3]

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 data protection and there are privacy-related events organised on a daily basis. Public awareness of privacy is high and likely increasing, owing to the fact that the GDPR is directly applicable. The ePrivacy regulation is also likely to increase this awareness.

Apart from that, new legislation supplementing the Act on the National Cybersecurity System, which transposed the NIS Directive into the Polish legal framework, was enacted during the past year. From many perspectives, and for different reasons, privacy is currently a matter of common concern and is expected to be even more crucial in the near future.

II THE YEAR IN REVIEW

2019 was very busy for Poland from a privacy-law perspective due to regulatory actions of the supervisory authority, as well as its issuance of several guidelines related to the implementation of the GDPR.

The first GDPR-related enforcement action in Poland's history took place on 15 March 2019, when the Polish supervisory authority (PUODO) issued its decision on one of the data controllers. The decision was focused on transparency obligations and – as argued by the regulator – resulted from not fulfilling the information obligations based on Article 14, Sections 1 and 2 of the GDPR. The controller at hand processed more than 7.59 million

2 The Act of 21 February 2019 on amending certain acts in order to ensure enforcement of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

3 www.politico.eu/pro/starving-watchdogs-will-police-eu-biggest-privacy-law-general-data-protection-regulation-europe/.

records about individuals conducting business activity or representing the legal entities (e.g., members of the board). The data was collected from public registers, available to everyone. The controller argued that it may rely on the exemption from the information obligations as provided in Article 14, Section 5(b) – the disproportionate effort, related to the time and cost of providing all the data subjects with information notices. The PUODO, however, did not agree with this position and imposed a €220,000 fine. What is more, the PUODO ordered the controller to inform all the data subjects in line with Article 14 Sections 1 and 2 within three months of receiving the decision by the controller. The controller appealed to the court and it is now expected that the case should be decided by the court at the beginning of 2020.

At the same time, the PUODO issued several interesting guidelines. For example, one focused on Brexit and transferring personal data to the UK after it leaves the EU.[4] The second describes the regulator's approach to data breaches.[5] Further, the PUODO issued a list of cases where a data protection impact assessment (DPIA) is mandatory for data controllers.[6]

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

Privacy law has its roots in the Constitution of the Republic of Poland of 2 April 1997,[7] 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 Polish Civil Code,[8] which protect the personal interests of natural persons.

Poland implemented EU Directive 95/46/EC[9] by enacting the Act of 29 August 1997 on the Protection of Personal Data (the Act on the Protection of Personal Data).[10] 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 the Protection of Personal Data (from 1997) is not binding from 25 May 2018, when the GDPR became fully effective.

Currently personal data protection is primarily governed by the GDPR. Nevertheless, there was a need to enact local law in order to adjust the Polish legal system to the requirements envisaged in the GDPR. The Act,[11] covering mostly institutional and organisational matters, such as the functioning of the PUODO and the rules of procedure in case of infringement of personal data protection laws, was adopted on 10 May 2018.

It shall be noted that many Polish sector-specific regulations contain provisions regulating personal data protection issues, such as in the laws governing banking, insurance, telecommunications, health and e-commerce. These sector-specific regulations also needed to

4 https://uodo.gov.pl/pl/383/665.

5 https://uodo.gov.pl/pl/file/2210.

6 http://monitorpolski.gov.pl/MP/2019/666.

7 Available in English at: www.sejm.gov.pl/prawo/konst/angielski/kon1.htm.

8 The Act of 13 April 1964 – Civil Code.

9 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 (http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046).

10 Available in English at: www.giodo.gov.pl/en/408/171.

11 The Act of 10 May 2018 on the Protection of Personal Data.

be amended to the extent necessary to ensure that they are fully compliant with the GDPR. The Derogation Act, which introduced changes to almost 170 Polish acts, entered into force on 4 May 2019.

The PUODO is quite active when it comes to enforcement actions and inspections. According to the PUODO's statement, it conducted more than 80 inspections under the GDPR and more than 4,500 data breaches were reported between 25 May 2018 and 25 May 2019.[12]

ii General obligations for data handlers

A controller, when processing personal data, must 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; 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 the PUODO of the data protection officer's appointment and provides contact details. The Act specifies that a person previously functioning as an information security administrator (under

12 https://niebezpiecznik.pl/post/pierwszy-rok-rodo-zgadnijcie-ile-razy-administratorzy-uchylili-sie-od-informowania-o-wycieku/.

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.

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 Data subject rights

Data subjects' rights are envisaged in the GDPR, such as the right to access (Article 15 of the GDPR), right to rectification (Article 16 of the GDPR), right to erasure (Article 17 of the GDPR), right to restriction of processing (Article 18 of the GDPR), right to data portability (Article 20 of the GDPR), right to object (Article 21 of the GDPR) and rights related to automated decision making and profiling (Article 22 of the GDPR) on the conditions determined therein.

According to Article 23 of the GDPR, the EU or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the rights and obligations provided for in, among others, Articles 15–22 of the GDPR. The Polish legislator decided to introduce such restrictions with regard to, for example, business information, by limiting the right to restriction of processing and excluding the right to object,[13] as well as with regard to processing carried out for journalistic purposes, by excluding the right to access, right to rectification, right to restriction of processing, right to data portability, right to object and the rights related to automated decision making and profiling.[14]

There have not been any specific laws enacted on enforcement of data subjects' rights in Poland. Nevertheless, such laws may be introduced in the future.

iv Specific regulatory areas

One of the most challenging aspects of the processing of personal data in Poland relates to the employer–employee relationship. It used to be common practice of Polish employers to process as much data of employees and candidates as possible. After the GDPR became directly applicable, this area has been regulated by the Polish regulations implementing the GDPR into the legal system (i.e., the Act and the Derogation Act, which have introduced amendments to the Polish Labour Code).[15]

The Polish legislator decided to clarify doubts that have arisen among employers after the GDPR became fully effective and explicitly indicated the legal grounds for processing of employees' and candidates' personal data. The Polish Labour Code now contains a catalogue of personal data that shall be requested by the employer from employees or candidates (the catalogue is different for each category).[16] In such cases, the personal data is processed on the basis of Article 6(1)(c) of the GDPR (legal obligation). Other categories of personal data, not included in the aforementioned catalogue, may be requested by the employer in case

13 Article 3 of the Act of 9 April 2010 on sharing business information and exchange of business information.

14 Article 2, Section 1 of the Act on the Protection of Personal Data.

15 The Act of 26 June 1974 - Labour Code.

16 Article 22(1), Section 1 and 3 of the Act of 26 June 1974 - Labour Code.

it is necessary to exercise a right or fulfil an obligation envisaged in applicable laws (e.g., background checks with regard to criminal records in case of public officials or regulated professions).[17] Candidates and employees shall disclose their personal data to the employer by means of declaration; however, the employer may request them to provide relevant documentation, to the extent necessary for its confirmation.[18]

According to the Polish Labour Code, candidates' and employees' personal data may also be processed on the data subject's consent, on the basis of Article 6(1)(a) of the GDPR, except for categories specified in Polish Labour Code, which shall be processed on the basis of Article 6(1)(c) of the GDPR (legal obligation) and personal data referred to in Article 10 of the GDPR (personal data related to criminal convictions and offences).[19] This encompasses both personal data disclosed by the candidate or employee on the employer's request and personal data shared on the initiative of the candidate or employee.[20] As to the special categories of personal data referred to in Article 9(1) of the GDPR ('sensitive personal data'), the candidate's or employee's personal data may be processed only in case they are shared on the candidate's or employee's initiative.[21] In line with the general requirements regarding consent envisaged in the GDPR, Polish Labour Code states that lack of consent or its withdrawal by the candidate or employee cannot constitute a ground for less favourable treatment of the candidate or employee nor can it result in any negative consequences for him or her, in particular it cannot constitute a reason for refusal to employ a candidate or to terminate an employment agreement with the employee.[22]

Although it has not been expressed in the Polish Labour Code, there is a general view that the explicit indication of the above-mentioned legal grounds for processing does not prohibit employers from relying on other legal grounds for processing, such as legitimate interest (Article 6(1)(f) of the GDPR), provided that the processing is fully compliant with the GDPR. Such conclusion has also been expressed in an explanatory memorandum issued by the Polish government.

The Polish Labour Code has also been amended by the Act on amending certain acts due to the reduction of the retention of employment records and their digitalisation,[23] which came into force on 1 January 2019 and aimed to meet the needs of Polish companies facing advancing digitisation. This act has, in particular, reduced the retention period of employment records from 50 years to 10 years (though it may differ in specific cases) and allowed the employers to decide whether they want to keep the employment records in paper or in electronic form (prior to the changes the employers were obliged to keep the employment records in paper form at all times).

17 Article 22(1), Section 4 of the Act of 26 June 1974 - Labour Code.

18 Article 22(1), Section 5 of the Act of 26 June 1974 - Labour Code.

19 Article 22(1a), Section 1 of the Act of 26 June 1974 - Labour Code.

20 Article 22(1a), Section 3 of the Act of 26 June 1974 - Labour Code.

21 Article 22 (1b), Section 1 of the Act of 26 June 1974 - Labour Code.

22 Article 22(1a), Section 2 of the Act of 26 June 1974 - Labour Code.

23 The Act of 10 January 2018 on amending certain acts due to reduction of the retention of employment records and their digitalisation.

v Technological innovation

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:[24]

a 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;

b the user, after receiving this information, consents to this use of his or her data; and

c 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.[25]

Location tracking

In July 2017, GIODO (now PUODO) published a broad analysis of the impact of location tracking on privacy.[26] The analysis covers both the Act 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,[27] expediency,[28] adequacy,[29] substantive correctness,[30] timeliness,[31] and integrity and confidentiality.[32] 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.[33]

24 Article 173, Section 1 of the Act of 16 July 2004 – Telecommunications Law.

25 Articles 209 and 210 of the Act of 16 July 2004 – Telecommunications Law.

26 Available at: http://giodo.gov.pl/pl/1520297/10068 (only Polish version).

27 Article 23, Section 1(1) of the Act on the Protection of Personal Data.

28 Article 23, Section 1(2) of the Act on the Protection of Personal Data.

29 Article 26, Section 1(3) of the Act on the Protection of Personal Data.

30 Article 26, Section 1(3) of the Act on the Protection of Personal Data.

31 Article 23, Section 1(4) of the Act on the Protection of Personal Data.

32 Article 36 of the Act on the Protection of Personal Data.

33 Available at: http://giodo.gov.pl/pl/1520297/10068 (only Polish version).

Electronic marketing

In terms of the Polish law regarding unsolicited commercial information, the rules of using electronic devices for marketing purposes remain 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.[34] 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 a prohibition on the use of telecommunication devices or automated calling systems for direct marketing.[35] 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, which coupled with the requests for consent for processing of personal data required on the basis of the GDPR, cause annoyance and lack of understanding on the part of the users.

The Derogation Act amended the relevant, abovementioned laws, i.e. the Act on Provision of Services by Electronic Means and the Telecommunications Law. The most significant change deriving from these amendments is that currently the consent to receiving commercial information by electronic means and the consent to direct marketing performed by means of telecommunication devices or automated calling systems shall fulfil the general requirements regarding consent provided in the GDPR.[36]

The Act on Provision of Services by Electronic Means explicitly states that online service providers may process customer's personal data, which is not necessary for the provision of the services, on the basis of customer's consent. The Polish legislator has also indicated the purposes for which such data may be processed – marketing, market research, investigation of customers' behaviour and preferences (provided that the results of the latter would be used for improving the quality of the services).[37] It is not clear whether this provision prohibits the marketers, while processing customers' data for the aforesaid purposes, from relying on other legal basis, such as legitimate interest (Article 6(1)(f) of the GDPR).

The above-mentioned provisions are intended to limit spamming. 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.

The new rules on the use of electronic devices for marketing purposes are expected with the adoption of the EU ePrivacy Regulation.

34 Article 10 Section 1 of the Act of 18 July 2002 on Provision of Services by Electronic Means.

35 Article 172 Section 1 of the Act of 16 July 2004 – Telecommunications Law.

36 Article 4 of the Act of 18 July 2002 on Provision of Services by Electronic Means; Article 174 of the Act of 16 July 2004 – Telecommunications Law.

37 Article 18, Section 4 of the Act of 18 July 2002 on Provision of Services by Electronic Means.

III 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 the matter of data transfer safeguards in Poland, when applicable, for the purpose of transferring personal data. Businesses operating in Poland often decide to implement standard contractual clauses or binding corporate rules, as well as some of them are a part of Privacy Shield Programme.

However, it should be noted that data transfer itself may be subject to restrictions arising from national legislation, depending on the specific area in which the company is operating. Such restrictions arise for example from banking law, where approval of the Polish Financial Supervision Authority is required when banking activities are outsourced to an entity having its registered office outside the European Economic Area.[38]

IV COMPANY POLICIES AND PRACTICES

i Non-mandatory character

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, adopting an online privacy policy became a common business practice among Polish online and e-commerce businesses. Many Polish companies, especially corporations, decided to introduce internal corporate privacy policies and internal privacy policies regarding employee rights and responsibilities. Moreover, a development and expansion of compliance and privacy departments in companies can be observed. In a number of cases, it is due to the obligation to appoint a data protection officer (DPO) deriving from Article 37 of the GDPR. However, many Polish companies decide to appoint a person responsible for privacy and data protection issues, although they are not required to do so by applicable laws.

ii Employee monitoring policies

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; or (4) protect the trade secrets, which disclosure might cause damage to the employer.[39] 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 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.[40] 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, the employer

38 Article 6d, Section 1 and Article 4, Section 3 of the Act of 29 August 1997 – Banking Act.

39 Article 22(2), Section 1 of the Act of 26 June 1974 - Labour Code.

40 Article 22(2), Section 3 and Section 4 of the Act of 26 June 1974 - Labour Code.

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.[41]

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.[42]

The Polish legislator decided to regulate also the issue of email correspondence surveillance conducted by the employers,[43] 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.

V 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.[44] Disclosing personal data to such authorities by Polish institution requires their initial verification as to accuracy and completeness. A disclosing institution may impose certain requirements on data receivers, such as removing personal data after a certain time or limiting the scope of personal data processed.

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 Border Guard, the Central Anti-Corruption Bureau and the Polish Military Police.

41 Article 22(2), Section 1(1) and Section 2 of the Act of 26 June 1974 - Labour Code.

42 Article 22(2), Section 6 – 10 of the Act of 26 June 1974 - Labour Code.

43 Article 22(3) of the Act of 26 June 1974 - Labour Code.

44 Act of 16 September 2011 on Exchanging Information with the Law Enforcement Authorities of the EU Member States, Third States, Agencies of the EU and International Organisations.

VI 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 an inspection. The scope of control is also limited as to its time frame, 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

The first fine of 943,470 zlotys for the infringement of the Article 14(1)–(3) of the GDPR was imposed due to the failure to inform data subjects about processing of their personal data.

The fined company processes personal data obtained from publicly available sources, including public registers, for commercial purposes. In its databases, there were over 7 million records of natural persons, including personal data of individual entrepreneurs, shareholders or members of relevant bodies of legal persons. When fulfilling obligations arising from the GDPR, the company provided the privacy notice to those data subjects, whose email addresses were publicly accessible in its database (as it is possible to conceal e-mail addresses and less than 1 million of the data subjects opted to have it accessible and others also provided phone numbers), but did not provide privacy notices via post for all other data subjects. In the company's opinion, fulfilling this obligation would have resulted in disproportionate effort and would have entailed an amount equal to the annual turnover for FY 2018. Thus, the company decided to publish the full version of the privacy notice on its website.

The PUODO found that this action was insufficient – while having other contact data (postal addresses and telephone numbers) for some of the data subjects, the controller should

have fulfilled the obligations arising from Article 14 of the GDPR toward entrepreneurs currently conducting business activity or those who conducted such activity in the past, as well as toward entrepreneurs who suspended it.

When imposing the fine, in its announcement, the PUODO emphasised that the amount of the fine was caused by the fact that the infringement of the controller was intentional – the company was aware of the obligation to provide data subjects with the relevant information, as well as the need to inform them directly. The PUODO indicated also that it took into account the fact that the controller did not take any action that would eliminate the infringement, nor did it declare such intention.

The second fine of 55,750.50 zlotys for the infringement of Article 5(1)(f), Article 32 (1)(b) and Article 32(2) of the GDPR was imposed for failure to ensure the security and confidentiality of processed data.

One of the Polish football associations made public on its website the personal data of football referees to whom licences had been granted. Apart from personal data such as their names, residence addresses and personal identification numbers were also published. The infringement affected 585 natural persons, was notified to the PUODO by the association and finally eliminated. However, as the PUODO indicated in its announcement, the controller took limited actions to eliminate the infringement, outsourced it to an external entity and did not verify the final result. This fact was decisive in the matter of imposing the fine on the association.

PUODO emphasised also that when deciding on the amount of the fine, the duration of the infringement and the number of people affected were taken into account, which in its opinion was large. However, the fact that there was no evidence on damage suffered by the data subjects affected and the association cooperated with the PUODO in the course of proceeding were mitigating factors.

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 one interesting case concerning smog and the overall air quality; the government was successfully sued based on the infringement of privacy and moral rights. The claimant argued that the government was obliged to take necessary steps to improve the quality of the air, and that by not doing so it invaded the citizen's private life and caused personal injury.[45]

VII 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

45 Press publication available at: https://www.rp.pl/Dobra-osobiste/301249966-Sad-smog-narusza-dobra-osobiste-Wyrok-z-powodztwa-aktorki-Grazyny-Wolszczak.html (only Polish version).

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.

In regard to data transfer matters, foreign organisations shall take into account above-mentioned considerations on restrictions of international data transfer.

VIII 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 August 2018 it was signed by the President of Poland and is now binding.

The purpose of this act is in particular to organise the national cybersecurity system and to indicate tasks and duties of the entities included in the Polish cybersecurity system. The system imposes different obligations on the operators of essential services, digital service providers, public entities a well as CSIRT MON, CSIRT NASK and CSIRT GOV. However, not all business entities are subject to the new regulation. Operators of essential services are entities, to whom the decision on recognising them as an operator of essential services was issued and those which belong to the sector and subsector indicated in Appendix 1 to the Act on the National Cybersecurity System. Appendix 1 indicates, among others, entities from the energy sector, transport service providers, entities providing banking services or healthcare services. The list of essential services was further specified in an executive regulation issued by the Council of Ministers.[46] The operators are obliged to recognise, register, analyse and take measures to remedy incidents that could endanger the cybersecurity. For the purpose of prevention, they shall collect all possible information about cybersecurity threats and apply preventive measures limiting occurrence of incidents.

The operators of essential services are also obliged to designate a contact person responsible for communication with entities within the national cybersecurity system. Moreover, it is necessary for them to carry out an audit of the security of the IT systems used for the purpose of providing essential service – at least once every two years.

The category of digital service provider involves legal persons or organisational units without legal personality, having its registered office or management on the territory of Poland or representatives with an organisational unit in Poland that provide digital services. Exceptions to the above are microentrepreneurs and small entrepreneurs within the meaning of the Entrepreneurs' Law.[47] Digital services – in accordance with Appendix 2 to the Act on the National Cybersecurity System – are online marketplace, cloud computing service and online search engine. The obligations of digital service providers are narrower than the obligations of operators of essential services.

Public entities that fall within the scope of the Act on the National Cybersecurity System are exhaustively listed in the act or specified in regulations on specific areas, such as public finance.

46 Regulation of the Council of Ministers on the list of essential services and thresholds on the significance of a disruptive effect of incident on the provision of essential services as of 11 September 2018.

47 Act of 6 March 2018 r. - Entrepreneurs' law.

In the scope of their services, entities within the cybersecurity system have 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 maintain an IT system through which the controllers shall be able to notify data breaches, though notification by post is also allowed.[48]

Therefore, on the PUODO's website there is an electronic form available, which is intended to be used while notifying a data breach, along with instructions for the controllers. It should be stressed 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 check boxes. 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, to settle official matters by electronic means in Poland it is necessary to aquire a trusted profile or electronic signature supported by a qualified certificate is necessary.[49] A trusted profile is a free-of-charge method of confirming identity in electronic contacts with Polish administration and some banks synchronised their systems to allow identification for the profile via online banking profiles. It can therefore be assumed that the electronic procedure of notifying data breaches will enjoy wide popularity among Polish entrepreneurs.

IX OUTLOOK

Businesses in Poland are waiting for the next guidelines from the regulator – in particular related to the execution of data subjects' rights. Some should also be issued by the Ministry of Digital Affairs, as several expert working groups created by the Ministry have been preparing

48 As confirmed by the PUODO's official mini guide to breach notification https://uodo.gov.pl/pl/134/233.

49 Available in English at: https://www.biznes.gov.pl/en/e-uslugi/00_0889_00.

GDPR white papers. Business will likely see further enforcement actions, in particular in relation to data breaches, which are quite common. It seems that the market expects strong messages from the regulator in this field – significant fines are therefore inevitable.

What is interesting is that few sectors expect their codes of conduct to be accepted by the PUODO. This includes the banking, internet advertising and healthcare sectors that are now working on the draft codes.

Further, we will see what impact Brexit will have on transferring personal data to the UK, as well as whether the EU Model Clauses and Privacy Shield will remain in force after the *Schrems 2.0* case.

Chapter 20

RUSSIA

Vyacheslav Khayryuzov[1]

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. 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

1 Vyacheslav Khayryuzov is a counsel at Noerr.

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, since an additional authorisation for transfers to certain countries may be necessary;

c have a data transfer agreement for any third-party transfers;

d have a primary database in Russia for personal data of Russian citizens;

e comply with technical requirements of the FSB and FSTEK, as well as Decree No. 1119;

f perform an internal data protection audit once every three years;

g adopt internal regulations on personal data protection and a privacy policy;

h appoint a data privacy officer;

i handle requests of individuals;

j define potential threats to personal data subjects;

k acquaint its employees with the internal data protection processes and regulations, and conduct training sessions on personal data security; and
l 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 Data subject rights

Data operators are required to handle requests by individuals with respect to the access, correction and deletion of personal data and are generally required to comply with requests by individuals relating to their personal data, unless there is an overriding mandatory statutory provision allowing the operator to continue processing the personal data.

As a part of the Personal Data Law, operators are obliged to notify individuals and the DPA of a resolved breach if a breach was found by an individual or the DPA and they requested that the breach be resolved. Data operators must notify individuals whose data was breached if the request to resolve the breach comes from them. The wording of the Personal Data Law assumes that such notices need to be personal and thus publishing a post or notice may not suffice. Furthermore, if the post or notice contains the personal data of the individuals affected, this would constitute a separate data breach.

iv 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.

v 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 localise 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 14 January 2019) includes Angola, Argentina, Australia, Benin, Canada, Chile, Costa Rica, Gabon, Israel, Japan, Kazakhstan, Malaysia, Mali, 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.

In most cases obtaining consent would be necessary in order to transfer personal data to a third party. 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 complicated 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 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 from using its IP address, which appears to be an ineffectual strategy. So far, the chase continues and Telegram is still available despite the DPA's actions.

On 3 June 2019, the well-known dating app Tinder was added to the register of messaging services. The owners of the app refused to share data with FSB,[2] saying that they registered because they have to comply with the local legislation. Since the law assumes provision of information to FSB, it remains to be seen how the situation will develop in the future.

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. Russia is taking steady steps to protect its internet infrastructure. 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

2 Link: https://www.themoscowtimes.com/2019/06/04/tinder-denies-sharing-russian-users-data-with-fsb-a65864.

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.

On 16 April 2019 Russia adopted the Runet Isolation Law. It will come into force on 1 November 2019. Under this law, the DPA will receive broad powers to control the internet. Furthermore, communications operators will be obliged to use traffic exchange points from a specially created registry run by the DPA, which should be physically located only in the territory of Russia. In addition, communications operators will be obliged to provide the DPA with all information about their network addresses, telecommunications message routes, software and hardware tools used to resolve domain names and communications network infrastructure.

Such a closed environment would make it easier to block any prohibited or unwanted services. The general idea of this law is to keep the Russian segment of the internet technically live even if it is switched off from the rest of the worldwide web (irrespective of whoever decides to do this – an external force or the Russian government itself). The blocking part also looks fairly logical, since it is currently difficult for the authorities to enforce blocking when illegal services are hosted by foreign-based providers. In a Russia-locked environment this would be much easier to do as all players would be only Russian companies and individuals.

It remains to be seen how this law would affect any foreign companies doing business in Russia. However, in the event of a doomsday scenario where the Russian segment is switched off from the rest of the web, it would certainly affect everyone working with Russia. From our perspective, however, this law is a kind of loaded gun that the authorities want to have 'just in case' and it does not seem likely that they would initiate the switch-off themselves.

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.

Russia recently signed the Protocol to the Council of Europe Convention No. 108. Therefore, we expect new amendments to the Personal Data Law that would harmonise the law with Convention No. 108. In particular, we expect the breach notification rules to be introduced. Furthermore, rules on depersonalisation would also cover commercial entities (up to now the DPA was of the opinion that only governmental entities were allowed to perform depersonalisation). There is also a draft law that would increase the fines for failure to localise personal data in Russia. The proposed maximum fine would be 18 million roubles. In April 2019, the DPA fined Twitter and Facebook for a failure to provide information on their compliance with data localisation rules. Both companies responded; however, as we understand it, the DPA was not satisfied with the responses and may still decide to block both social networks in Russia.

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[1]

I OVERVIEW

In 2018 and 2019, Singapore continued to develop its data protection, cybercrime, and cybersecurity regimes. As set out in Singapore's Cyber Landscape 2018 report,[2] the government focused on four pillars of strategy to protect the country from cyberthreats and reinforce Singapore's standing as a leading information systems hub. It aimed to: (1) build a resilient infrastructure; (2) create a safer cyberspace environment; (3) develop a vibrant cybersecurity ecosystem; and (4) strengthen international partnerships. 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 Cybersecurity Act, which focuses on protecting Singapore's Critical Information Infrastructure (CII) in 11 critical sectors 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.

---

1 Yuet Ming Tham is a partner at Sidley Austin LLP.

2 See Singapore's Cyber Landscape 2018, Cybersecurity Agency of Singapore, available at https://www.csa.gov.sg/~/media/csa/documents/publications/csasingaporecyberlandscape2018.pdf.

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 10 months from August 2018 to June 2019.

On 31 August 2018, the PDPC concluded public consultation on Proposed Advisory Guidelines on the PDPA for national registration identity cards (NRIC) numbers and issued updated advisory guidelines on the PDPA for NRIC and other national identification numbers. The advisory guidelines attempt to enhance consumer protection against indiscriminate collection, use and disclosed of individuals' NRIC numbers and retention of physical NRICs. All organisations must comply with the updated advisory guidelines beginning 1 September 2019.

On 23 January 2019, the PDPC presented the first edition of a proposed model artificial intelligence (AI) governance framework for public consultation and pilot adoption. The accountability-based framework orchestrates discussions around harnessing AI in a responsible way by creating guidelines by which organisations can deploy AI solutions responsibly. Public consultation was welcome on this topic until 30 June 2019.

The PDPC released a discussion paper on the benefits of data portability in late February 2019, signalling an intent to address data portability in future PDPA amendments. Data portability allows individuals to have greater control over their personal data by requesting copies of their data held by an organisation in a commonly used format, as well as requesting that the organisation transmit the data to another organisation. The PDPC then issued a public consultation on a proposed data portability and data innovation provision from 22 May 2019 to 3 July 2019. The proposed data portability provision would provide individuals with increased control over their personal data and enable access to more data by companies to facilitate data flows and increase innovation, while the proposed data innovation provision clarifies that companies can use personal data for business purposes without individuals' consent.

The PDPC issued a statement on 1 March 2019 confirming its intent to introduce a mandatory breach notification regime as part of proposed amendments to the PDPA. The proposed notification mandate would require organisations to notify both affected individuals and the PDPC when a data breach risks harm to individuals involved in the breach, as well as notify the PDPC regardless of potential impact when there has been a significant data breach (i.e., more than 500 individuals' personal data is affected). This proposal received widespread public support during recent public consultations from July to October 2017.

The PDPC issued a Guide on Active Enforcement and Guide to Managing Data Breaches 2.0 on 22 May 2019 (collectively, the Guides), which detailed the PDPC's approach to regulating Singapore's data privacy regime. The Guides provide a roadmap to help organisations develop data breach management plans that can identify data protection concerns early, increase awareness of data protection across the entire organisation, and comply with Singapore's data protection principles. Significantly, the Guide to Managing Data Breaches 2.0 states that companies should inform the PDPC of certain data breaches within 72 hours of the breach. This timeline is consistent with the mandatory notification prescribed under the European Union's General Data Protection Regulation (GDPR).

Singapore and Hong Kong signed a memorandum of understanding (MOU) to strengthen cooperation in personal data protection at the 51st Asia Pacific Privacy Authorities Forum. The MOU was signed by Mr Stephen Kai-yi Wong (Hong Kong's Commissioner for

Personal Data) and Mr Yeong Zee Kin (Deputy Commissioner of Singapore's Personal Data Protection Commission). Stemming from this cooperative MOU, Hong Kong and Singapore jointly released a Guide to Data Protection by Design for ICT Systems on 31 May 2019.[3]

ii CMCA developments and the Cybersecurity Act

The CMCA and the Cybersecurity Act are closely linked. In Singapore's October 2016 cybersecurity strategy report, the government noted the need for a comprehensive framework to prevent and manage the increasingly sophisticated threats to Singapore's cybersecurity.[4] 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), which was previously issued for public consultation on 10 July 2017. The Cybersecurity Act ultimately came into effect on 31 August 2018. The Cybersecurity Act creates a framework for the protection of CII against cyberthreats, creates the Commissioner of Cybersecurity with broad powers to administer the Cybersecurity Act, establishes a licensing scheme for providers of certain cybersecurity services, and authorises measures for the prevention, management, and response to cybersecurity incidents in Singapore.

Under Section 2 of the Cybersecurity Act, 'cybersecurity' is defined as the state in which a computer or system is protected from unauthorised access or attack and, because of that state: (1) the computer or system continued to be available and operational; (2) the integrity of the computer or system is maintained; or (3) the integrity and confidentiality of information stored in, processed by or transmitted through the computer or system is maintained. 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

3 See Guide to Data Protection by Design for ICT Systems (31 May 2019), available at https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Data-Protection-by-Design-for-ICT-Systems-(310519).pdf.

4 See Singapore's Cybersecurity Strategy, Cybersecurity Agency of Singapore (October 2016) (Cybersecurity Report).

but not limited to, reporting to the Commissioner certain prescribed incidents, establishing mechanisms and processes for detecting cybersecurity threats and incidents, reporting any material changes to the design, configuration, security or operation of the CII, complying with all codes of practice and standards of performance issued by the Commissioner, conducting regular audits of compliance of the CII with the Cybersecurity Act, and participating in cybersecurity exercises as required by the Commissioner.

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.

Cross-border enforcement of the Cybersecurity Act poses a challenging problem, particularly for cloud-based service providers. Singapore signed several MOUs with multiple foreign governments to signal their desire for international collaboration to address cybersecurity. These MOUs were with Australia, Canada, India, France, the Netherlands, the United States and the United Kingdom. Singapore additionally signed a Joint Declaration on Cybersecurity Cooperation with Germany and a Memorandum of Cooperation on Cybersecurity with Japan.

iii 2019 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]

Singapore experienced its most serious data privacy breach yet in July 2018 when hackers infiltrated Singapore Health Services' (SingHealth) databases, compromising the personal data of 1.5 million patients, including the outpatient prescriptions of Prime Minister Lee Hsien Loong. The PDPC fined Integrated Health Information Systems (the IT agency responsible for Singapore's public healthcare sector) S$750,000 and SingHealth S$250,000 for breaching their data protection obligations leading to the breach.

5 Government agencies are not covered by the scope of the PDPA.

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 mediums. 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 years[10] and personal data contained within records for over 100 years is exempt.[11]

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]

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.
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.

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.

Consent[23]

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.[24] 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.[25]

Purpose limitation[26]

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.

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.

26 Section 18 of the PDPA.

Notification[27]

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.[28]

Access and correction[29]

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.[30]

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.[31]

Accuracy[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[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.[34]

Retention limitation[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.

27 Section 20 of the PDPA.

28 PDPC Guide to Notification, issued on 11 September 2014.

29 Sections 21 and 22 of the PDPA.

30 Section 22(6) and Sixth Schedule of the PDPA.

31 15.18, PDPA Key Concepts Guidelines.

32 Section 23 of the PDPA.

33 Section 24 of the PDPA.

34 See discussion in Sections 17.1–17.3, PDPC Key Concepts Guidelines.

35 Section 25 of the PDPA.

Transfer limitation[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[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 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.[38] Where cookies used for behavioural targeting involve the collection and use of personal data, the individual's consent is required.[39] 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.[40] 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

36 Section 26 of the PDPA.

37 Sections 11 and 12 of the PDPA.

38 Sections 7.5–7.8, PDPA Selected Topics Guidelines.

39 Section 7.11, PDPA Selected Topics Guidelines.

40 Section 9(4)(a) of the Personal Data Protection Regulations 2014.

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.[41]

iv Specific regulatory areas

Minors

The PDPA does not contain special protection for minors (under 21 years of age).[42] 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.[43] The Education Guidelines[44] 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),[45] the country's central bank and financial regulatory authority, require various financial institutions to, among other things:

a 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

b 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.

41 Section 12.61, PDPA Key Concepts Guidelines.

42 Section 8.1, PDPA Selected Topics Guidelines.

43 Section 14(4) of the PDPA. See also discussion at Section 8.9 of the PDPA Selected Topics Guidelines.

44 Sections 2.5–2.8, PDPC Advisory Guidelines on the Education Sector, issued 11 September 2014.

45 MAS Notice SFA13-N01 regulating approved trustees; MAS Notice 626 regulating banks; MAS Notice SFA04-N02 regulating capital markets intermediaries; MAS Notice FAA-N06 regulating financial advisers; MAS Notice 824 regulating finance companies; MAS Notice 3001 regulating holders of money-changers' licences and remittance licences; MAS Notice PSOA-N02 regulating holders of stored value facilities; MAS Notice 314 regulating life insurers; MAS Notice 1014 regulating merchant banks; and MAS Notice TCA-N03 regulating trust companies.

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 now 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[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.[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

46 Section 6 of the PDPC Healthcare Guidelines.

47 Paragraph 1(o) Second Schedule, Paragraph 1(j) Third Schedule, and Paragraph 1(s) Fourth Schedule of the PDPA.

potential employee to consent to, nor to be notified of, their collection, use or disclosure.[48] Other legal obligations, such as to protect confidential information of their employees, will nevertheless continue to apply.[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.

S/N	Area of protection	Recipient is:	
		Data intermediary	Organisation (except data intermediary)
1	Purpose of collection, use and disclosure by recipient	–	Yes
2	Accuracy	–	Yes
3	Protection	Yes	Yes
4	Retention limitation	Yes	Yes
5	Policies on personal data protection	–	Yes
6	Access	–	Yes
7	Correction	–	Yes

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.[50]

An organisation may transfer personal data overseas if:

a 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

b 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.[51] 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.[52]

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;[53] or where the transfer is necessary for the performance of a contract.

48 Paragraph 1(f) Second Schedule, Paragraph 1(f) Third Schedule and Paragraph 1(h) Fourth Schedule of the PDPA.

49 Sections 5.14–5.16 of the PDPA Selected Topics Guidelines.

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.

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.

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.[54]

The Key Concepts Guidelines[55] 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).

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.[56] Organisations must also develop a complaints mechanism,[57] and communicate to their staff the policies and practices they have implemented.[58] Information on policies and practices, including the complaints mechanism, is to be made available on request.[59] 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.[60]

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.

54 Regulation 9(2)(a) of the PDP Regulations.

55 Issued on 23 September 2013 and revised on 8 May 2015.

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.

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.

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 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

61 Section 4(6) of the PDPA.

69 Section 29 of the PDPA.

70 Section 55 of the PDPA.

71 Section 56 of the PDPA.

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, or is attributable to his or her neglect.[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.[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.[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.

ii Recent enforcement cases

In 2018, the PDPC published 29 decisions. By June 2019, the PDPC had already published 20 decisions. 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 2018 and the first half of 2019 set out the PDPC's typical mix of behaviour remedies combined with financial penalties, including:

a GrabCar Pte Ltd (June 2019):[75] PDPC issued a fine of S$16,000 to the organisation for failing to put in place reasonable security arrangements to protect the personal data of its customers from unauthorised disclosure. For example, personal data of a customer was disclosed to one other customer via an email sent out by the organisation.

b Matthew Chiong Partnership (June 2019):[76] PDPC issued a fine of S$8,000 for the organisation's failure to fulfil its protection obligation and openness obligation under the PDPA and directed the organisation to put in place a data protection policy to comply with the provisions of the PDPA.

c WTS Automotive Services Pte Ltd (December 2018):[77] PDPC issued a fine of S$20,000 to the organisation for failing to make reasonable security arrangements to prevent the unauthorised disclosure of its customers' personal data.

iii 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

72 Section 52 of the PDPA.

73 Section 53 of the PDPA.

74 Section 35 of the PDPA.

75 Decision Citation: [2019] SGPDPC 15.

76 Decision Citation: [2019] SGPDPC [7].

77 Decision Citation: [2018] SGPDPC 26.

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 accessing[80] 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.

79 www.pdpc.gov.sg/docs/default-source/advisory-guidelines-on-enforcement/advisory-guidelines-on-enforcement-of-dp-provisions-(210416).pdf?sfvrsn=2.

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 crime[85] 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. In December 2018, MAS launched a S$30 million Cybersecurity Capabilities Grant to enhance cybersecurity capabilities in the financial sector and assist financial institutions in developing local talent in the cybersecurity sector.

X OUTLOOK

In keeping with its declared strategy, Singapore continues to clarify and enforce 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.

Chapter 22

SPAIN

Leticia López-Lapuente and Reyes Bermejo Bosch[1]

I OVERVIEW

Cybersecurity and data protection are becoming essential values for society and, consequently, both areas have recently undergone significant legal development recently. In particular, a new law on cybersecurity and a new national data protection law were passed in the second half of 2018. Both laws are based on and mirror the corresponding EU Security of Network and Information Systems Directive (the NIS Directive) and the General Data Protection Regulation (GDPR). Nevertheless, data protection and privacy rules are more consolidated in the EU and Spain than cybersecurity regulations, which are still in need of further development.

Data protection and privacy are distinct rights under Spanish law, but both are deemed fundamental rights derived from the 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 not sufficiently developed yet.

With regard to data protection, as in all other EU jurisdictions, the main rule is the GDPR. That said, Spain approved the new Basic Law 3/2018 on Data Protection and digital-rights guarantees (the New Spanish Data Protection Law) on 5 December 2018, which entered into force on 7 December 2018. With the approval of this law, former Spanish data protection laws and regulations have been repealed.

In addition to the foregoing legal regime, there are sector-specific regulations that also include data protection provisions, since certain categories of personal data and certain processing activities may require specific protection such as the processing of personal data within the financial, e-communications or health-related sectors. There are several codes of conduct for data protection that were approved under the former Spanish data protection regulations for various sectors. These codes are being reviewed pursuant to the GDPR and the New Spanish Data Protection Law.

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

1 Leticia López-Lapuente and Reyes Bermejo Bosch are lawyers at Uría Menéndez Abogados, SLP.

expression) as well as other legitimate interests (e.g., intellectual property rights, public security and prosecution of crimes). In the case of data protection, this balance must be primarily assessed by the organisation and individuals, and public entities and other organisations may challenge the assessment 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 imposing significant sanctions. In 2018 alone, the DPA received 13,599 claims from individuals, organisations and authorities (including authorities of other EU jurisdictions) and issued and published 434 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.

II THE YEAR IN REVIEW

The New Spanish Data Protection Law was approved in December 2018. This was the most relevant data protection milestone in Spain over the past year. The New Spanish Data Protection Law was not enacted with the aim of implementing the GDPR, which is directly applicable in Spain since 25 May 2018. Instead, it aims to harmonise Spanish law with the provisions of the GDPR and to provide specific data protection regulation in different fields that are not expressly included in the GDPR or that are included in the GDPR but with a scope that allowed for more detailed regulations to be introduced by the Member States. This is the case, for instance, of the specific regulation in the New Spanish Data Protection Law on processing operations, such as those resulting from video-surveillance, whistleblowing schemes or the inclusion and consultation of debtors' data in credit bureaus.

Moreover, the New Spanish Data Protection Law incorporates into the Spanish legal system a list of new rights of citizens in relation to new technologies, known as 'digital rights'. These 'digital rights', which are not data protection rights as such but independent digital rights, can be divided into three categories:

a general rights aimed at all citizens, such as the right to the digital testament, to a digital education or to the digital security;

b specific rights addressed to providers of information society services and social networks, some of which seem as reaction to recent and significant public cases, such as the right to rectification or update of information over the Internet or the right to be forgotten; and

c specific rights closely related to the use of technologies within the employment relationships, such as the right to privacy in the use of digital devices, of video surveillance and geo-localisation in the workplace. These rights present some limitations on the processing for these purposes and obligations for employers to inform employees about access to the information stored on digital devices supplied by the employer to the employees and for the use of video-surveillance systems and geo-localisation for the purposes of controlling employees. In addition, the novel 'digital disconnection right' is included, which aims to guarantee workers' and civil servants' break time, leave and holidays.

In addition, the New Spanish Data Protection Law also includes an amendment of Spanish General Electoral Law, allowing political parties to process of personal data for specific electoral promotional activities, though this amendment caused much debate and controversy and thus was recently annulled by the Spanish Constitutional Court (see Section VII.ii) below).

Regarding the implementation of the NIS Directive, the Spanish government approved a law (by approving a royal decree-law) (see Section IX), although a regulation to develop the law is yet to be approved.

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, Spanish courts have held that the right to be forgotten is a right distinctive from data protection rules, in line with the recognition of a digital right to be forgotten in the New Spanish Data Protection Law. More recently, on 11 January 2019, the Spanish Supreme Court issued a ruling regarding the scope and nature of the 'right to be forgotten'). The relevance of this ruling is that the Spanish Supreme Court has established certain limits on the right to be forgotten, recognising that freedom of information may prevail where the news is published by digital means and the news is accurate and refers to facts of public relevance or general interest.

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 the New Spanish Data Protection Law.

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, financial regulation or the regulations on clinical records or biomedical research. However, they generally refer to the former Spanish data protection regulations and, now that the GDPR and New Spanish Data Protection Law are in force, will either be subject to review or should at least be reinterpreted according to the new 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 minors, political opinions, trade-union membership, religion or philosophical beliefs, racial or ethnic origin, genetic data, biometric data, health, criminal offences, sex life or sexual orientation are deemed more sensitive and require specific protection. This protection is established in the GDPR in the regulation on the so-called 'special categories of personal data' or in specific and more restrictive rules for the processing of data of minors or data related to criminal offences. In addition to this additional protection granted in the GDPR, the New Spanish Data Protection states that the processing of data related to administrative offences also requires additional measures.

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 by both controllers and processors with the data protection duties imposed by the GDPR (fair information, legitimate ground, security, proportionality and quality, accountability, etc.)[2] and by the New Spanish Data Protection Law (direct-marketing processing activities, credit bureaus, whistle-blowing schemes, video-surveillance, etc.). The DPA has in the past carried out and *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). More recently, in 2019, it has carried out a specific analysis of Android devices regarding (1) access on the screen to applications for Android devices; (2) user controls for ad personalisation in Android; and (3) information flows in Android and tolls for compliance with accountability. 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 the New Spanish Data Protection Law 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). Section VII.i below explains how the New Spanish Data Protection Law has developed the general sanctioning regime set out in the GDPR. Neither harm nor injury is required for an administrative sanction to be imposed (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 for data subjects to claim damages arising from breaches of data protection rights before civil and criminal courts.

ii General obligations for data handlers

The main obligations of data controllers and data processors are those set out in the GDPR and in the New Spanish Data Protection Law, but sector-specific Spanish regulations may also provide specific rules on the processing of personal data in a specific sector or activity (e.g., data included in clinical records).

Obligations of data controllers

a Any processing activity should be internally monitored, registered and documented;

b data controllers must assess risks before implementing data processing operations and must ensure from the design of any processing operations that data protection principles and rules are met (i.e. privacy by design and privacy by default);

c 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);

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.

d 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;

e 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;

f controllers should adopt appropriate security measures and notify the DPA and, in some cases, the affected data subjects, of any data breaches, as explained in Section IX; and

g as explained in Section III.iii below, data subjects have specific rights concerning their personal 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);

e assist the controller by identifying any instructions that could infringe data protection rules and, if so agreed, assist in managing data protection requests from individuals;

f notify without delay any data breaches suffered that affect the controller's personal data;

g allow controllers to audit their processing; and

h upon termination of the services, return or destroy the data, at the controller's discretion.

iii Data-subject rights

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.

In addition, the New Spanish Data Protection Law establishes the obligation of the data controller to block the data during a reasonable term following rectification or erasure of the data, in order to prevent its processing but still have it available to judges and courts, the Public Prosecution Service or the competent public authorities (including the data protection authorities) in relation to potential liabilities derived from the processing and only during the applicable limitation period. Once the blocking period has ended, the data controller must delete the data.

As regards data subjects' right to obtain compensation for damage from data controllers or processors, the GDPR has reinforced the rights including the right of consumer organisations to bring class actions. The New Spanish Data Protection Law adds no significant changes to the general regime provided in the GDPR.

iv Specific regulatory areas

The data protection 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 for children under 14) 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). The New Spanish Data Protection Law incorporates – and comprehensively regulates – data processing activities that are not expressly regulated in the GDPR. This is the case, for example, of data processing activities for video-surveillance purposes, whistle-blowing channels and solvency and credit files. Some of these specific data processing activities were regulated in the former Spanish data protection regulations (e.g., solvency and credit files) or were the subject matter of specific guidelines by the DPA, in which case, in general, the New Spanish Data Protection Law continues in the same vein regarding those guidelines or previous national regulations.

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);

c 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);

d the use of genetic data or information contained in biological samples (Law 14/2007 of 3 July on biomedical research);

e information used for direct-marketing purposes (LSSI);

f 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

g 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 data protection regulations, after May 2018 they will need to be reviewed according to the GDPR or, at least, reinterpreted according to GDPR rules.

v Technological innovation

Technology has created specific issues in the privacy field, including:

a electronic-privacy issues, including for ISPs, online platforms, and search engines;

b 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);

c location tracking: the New Spanish Data Protection Law and the DPA consider that the use of this technology in work environments may be reasonable and proportionate provided that certain requirements and proportionality test are met (mainly, that specific information has been previously provided to data subjects on the potential monitoring of IT resources). At the beginning of 2019, the Spanish labour courts handed down a significant ruling in a case involving the Spanish company Telepizza (Sentence 13/2019 issued by the National Audience on 6 February 2019). The decision annulled the tracking systems implemented by the company because, among other things, they did not meet the information and proportionality requirements;

d 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 2018, the DPA received 1,353 claims and issued 55 sanctioning resolutions regarding internet services (certain of which included the use of cookies);

e biometrics: traditionally, the processing of biometric data has not been considered 'sensitive' and, therefore, the implementation of the GDPR in Spain implies a change in the concept of biometrics, which are now considered especially protected data. The DPA has issued a 'survey on device fingerprinting' and recent opinions on the lawfulness and proportionality requirements for the use of fingerprinting for attendance and schedule control purposes;

f big data analytics: in April 2017, the DPA published guidelines on how to implement big data projects according to GDPR rules;

g 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 and it has recently published a study regarding 'K-anonymity as a privacy measure';

h internet of things and artificial intelligence: the DPA has not adopted an official position regarding the internet of things and artificial intelligence, but it is currently working on those fields;

i 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;

j 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*,[3] 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 (see the

3 Case C-131/12.

ruling issued by the Spanish Supreme Court on 11 January 2019 mentioned in Section II). Also, 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 this was ultimately confirmed by the New Spanish Data Protection Law, which has included the right to be forgotten as one of its new digital rights; and

k 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 data protection rules prior to the GDPR, data transfers from Spain to (or access by) recipients located outside the EEA required the prior authorisation of the DPA, unless the transfer could be based on a statutory exemption.[4] However, this local regime was repealed by the GDPR and general rules in the GDPR applicable to international transfers of personal data apply directly in Spain. Also, the New Spanish Data Protection Law does not include changes to the GDPR's general regime. Thus, international transfers of personal data cannot be carried out unless they are made to white-listed countries, if specific safeguards are adopted (such as BCRs or EU Model Clauses) or if they are based one of the derogations of Article 49 of the GDPR.

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 Spanish 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).

To that end, organisations in Spain are adopting corporate privacy policies and cybersecurity prevention and reaction plans as part of their internal compliance programmes.

4 The DPA's prior authorisation is not required in the cases set out in Article 26 of EU Directive 95/46/EC.

Those policies not only comply with the above-mentioned duties but also evidence that principles such as privacy-by-design are duly implemented within the organisations. Approval at board and management level of these policies and strategies is also required, which thus reinforces the involvement of top management on data protection and cybersecurity matters.

ii Data protection officers

Before May 2018, a data protection 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. The New Spanish Data Protection Law expands and provides additional details on the cases in which the appointment of a data protection officer will be mandatory including, among others: financial entities, insurance and reinsurance companies, educational institutions, and private-security companies.

Under the former Spanish data protection regulations, the appointment of a security officer specifically in charge of implementation of security measures was required under certain circumstances, but from 25 May 2018, the appointment of this role is no longer mandatory.

iii Privacy impact assessments

Privacy impact assessments have been mandatory for certain data processing as from May 2018. For this reason, the DPA has published guidelines on how to carry out 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 Spain has recently published the 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). In addition, the DPA has designed an electronic tool (publicly available on its website) to carry out privacy impact assessments.

iv Data mapping

As part of the mandatory risk analysis, organisations should carry out data-mapping activities regarding the collection, use, transfer and storage of personal data. The DPA offers various electronic tools to help organisations in this regard; however, the use of such tools is intended for either small companies or companies that carry out simple processing activities.

v Work councils

Employee representatives – works councils and employee delegates – are entitled to issue a non-binding report before new methods of control of work are put into place or if existing methods are modified. Since what qualifies as a 'method of control' of work is sometimes debatable and unclear, it is generally advisable to inform the employee representatives of the implementation or modification of control methods (e.g., whistle-blowing systems or IT acceptable-use policies) and offer them the possibility of issuing the non-binding report.

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 (currently, the European Data Protection Board (EDPB)). 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 a 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[5] 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). It is worth noting that the New Spanish Data Protection Law has further developed the general and rather vague sanctioning regime set out in the GDPR, by providing, on the one hand, three categories of infringements (minor, serious and very serious) which depend on the type and seriousness of the breach – rather than the mere two fine ranges set out in the GDPR – and, on the other hand, a detailed administrative sanctioning and investigation system and procedures.

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 2018 (the most recent official statistics published by the DPA): 12,517 complaints from individuals were solved (which includes the 531 data breaches that were communicated but not investigated) and the fines imposed amounted to approximately €13.2 million. Most of the sanctions imposed on the private sector were for lack of consent and breach of the quality principle.

5 See footnote 2.

ii Recent enforcement cases

The following are the most significant enforcement issues to have arisen in Spain in the period 2018–2019.

The DPA has carried out numerous disciplinary proceedings related to video-surveillance (260), unlawful contracting (107) and the disclosure of data to solvency and credit agencies (105). The DPA has also issued several reports assessing the interpretation of both the GDPR and the New Spanish Data Protection Law, the new regulation applicable to political opinions or the application of the legitimate interest as a legitimate ground for the processing, including a legal report regarding commercial communications by non-electronic means.

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. The DPA has indicated that it has participated in 262 cases of cross-border cooperation.

Finally, the Spanish Constitutional Court has issued a significant ruling (ruling dated 4 June 2018) declaring the unconstitutionality of Section 1 of Article 58 *bis* of Basic Law on the General Electoral System (related to Article 56 of the GDPR). Article 58 *bis* was introduced by the Third Final Provision of the New Spanish Data Protection Law and refers to the processing of citizens' political opinions by political parties. In particular, the unconstitutional section provided that '[t]he collection of personal data relative to the political opinions of people that are carried out by political parties in the framework of their electoral activities will be covered by the public interest only when the appropriate guarantees are offered'.

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 is news in the market around the recent initiation by the Spanish consumers association of class actions related to alleged data protection 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 the 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.

There are some rules in Spain that require specific types of data (e.g., anti-money laundering, health data, specific financial records held by credit institutions or public archives, classified data relevant to national security) to be stored and processed within Spanish territory (unless an exception applies).

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. Spain was late in implementing the NIS Directive but in September 2018 a law was finally passed. In particular, the NIS Directive was implemented into Spanish law through Royal Decree-Law 12/2018 of 7 September, on the security of networks and information systems; however, Royal Decree-Law 12/2018 provides general and unspecific rules and a further regulation developing such aspects remains pending (a first draft of the Royal Decree has recently been published that develops Royal Decree-Law 12/2018, although its content is not necessarily final).

Royal Decree-Law 12/2018 is consistent with the NIS Directive and, in general, does not introduce particularities. Royal Decree-Law 12/2018 only applies to operators of essential services[6] located in Spain and digital service providers registered in Spain (provided that Spain constitutes its main establishment in the EU). Regarding the notification of security breaches, Royal Decree-Law 12/2018 proposes the creation of a common platform that could also be used to notify breaches of personal data security according to the GDPR (it has been included as part of the draft Royal Decree that will develop Royal Decree-Law 12/2018). However, at this time, breaches of personal data security are being notified through the online platform available on the DPA's website.

However, in addition to cybersecurity duties arising from the NIS rules, security and cybersecurity duties can be found in other Spanish rules. This means that the legal regime is rather disseminated and complex. We providea summary below.

For instance, the GDPR also establishes specific security duties for data controllers and processors when processing personal data, as well as notification duties in the event of data breaches. For this reason, the DPA is highly active in relation to cybersecurity matters. Following certain global attacks, the DPA has been publishing posts on its website regarding cyberattacks and how to guard against them. Among other recommendations, the DPA has 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. In addition, in 2018 and 2019, the DPA published guidelines regarding how to react in the event of data breaches including general guidelines on how to manage and notify data breaches.

6 They are mainly operators of critical infrastructure. More information below.

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 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. Also, the LSSI 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).

In addition to the obligations set out in Royal Decree-Law 12/2018, operators of critical infrastructure[7] (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

7 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.

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. The draft Royal Decree that will develop Royal Decree-Law 12/2018 has included the mandatory appointment of an information-security officer by operators of essential services. The draft provides a list of functions and responsibilities as well as a list of requisites to be complied with by the information security officer. The provisions included in the draft Royal Decree should prevail over the current framework under Law 8/2011; however, no derogative provisions have been included at this stage.

Furthermore, Spanish 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 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.

In addition to the above-mentioned laws, certain authorities with specific cybersecurity responsibilities have issued guidance, such as:

a the most recent guidelines published by the Spanish National Institute of Cybersecurity (INCIBE) regarding, inter alia:
- wi-fi network security (2019);
- back-up files (2018);
- increased competitiveness by complying with the GDPR (2018); and
- cloud computing (2017);

b the publication by INCIBE in 2016 of a consolidated code of cybersecurity rules in Spain (amended in June 2019);

c the National Cybersecurity Strategy issued by the presidency in April 2019;

d the strategy series on cybersecurity issued by the Ministry of Defence; and

e 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 competence in cybersecurity are numerous and include:

a the CCN, which is part of the National Intelligence Centre;

b the CCN Computer Emergency Response Team;

c the CNPIC;

d the Cybersecurity Coordinator's Office (which is part of the CNPIC);

e the Secretary of State for Digital Development; and

f INCIBE (previously known as the National Institute of Communication Technologies), which is the public-sector company in charge of developing cybersecurity.

Finally, also related to cybersecurity and security legal duties, Spanish legislation includes disseminated rules on data retention or deletion rules. Most of these rules are sector-specific

(e.g., AML rules establish retention duties of 10 years for certain information). However, the scope of some of these rules is more general and applies to the vast majority of companies in Spain, such as Article 30 of Spanish Commercial Code, which obliges companies to retain documentation with an impact on accounting for at least six years. More recently, the New Spanish Data Protection Law set out general retention rules, such as the one-month retention rule applicable to video surveillance.

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 to 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 recent approval of the New Spanish Data Protection Law represents a challenge for Spanish companies, which must deal not only with the GDPR provisions but also with the new set of particularities included by the New Spanish Data Protection Law that affect specific processing activities such as those involving solvency files, direct-marketing activities and video surveillance. Although the GDPR provides for data protection principles that are similar to those of the repealed Directive 95/46/EC and former Spanish data protection regulations, as construed by the CJEU and the EDPB, 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 occur in Spain in the coming months, particularly if the draft Royal Decree further developing some of the general rules set out in Spanish Royal Decree-Law 12/2018 is approved.

Chapter 23

SWITZERLAND

Jürg Schneider, Monique Sturny and Hugh Reeves[1]

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[2] (DPA) and the accompanying Swiss Federal Ordinance to the Federal Act on Data Protection of 14 June 1993[3] (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.[4] Accordingly, Swiss data protection law has some peculiarities that differ from the legal framework provided by the EU General Data Protection Regulation[5] (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.[6] 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 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.[7] 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 main data protection reform is quite significantly delayed compared to the initial schedule. The first step of the revision entered into force on 1 March 2019 with the adoption of the Schengen Data Protection Act of 28 September 2018[8] and some amendments to the DPA. The Schengen Data Protection Act is merely a provisional law, which shall be integrated entirely into the DPA in the course of the imminent second step of the reform (i.e., the main revision of Swiss data protection law). Once the revised DPA has entered into force, the Schengen Data Protection Act will be repealed. Entry into force of the second step comprising the remaining main revisions to Swiss data protection law is tentatively scheduled for 2020, although 2021 seems more realistic due to recent further delays in the parliamentary discussions.

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 19 July 2019). An unofficial English translation of the draft DPA can be found at: https://www.dataprotection.ch/user_assets/pdfs/Swiss_Data_Protection_Act__draft_of_September_2017__Walder_Wyss_convenience_translation_V010.pdf?v=1507206202 (last visited on 19 July 2019).

8 Classified compilation (SR) 235.3.

Subsequent to a revision process, the revised Swiss Federal Act on the Supervision of Postal and Telecommunication Services of 18 March 2016[9] and the revised related ordinance[10] entered into force on 1 March 2018.[11] 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.[12]

A revised 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.[13] The new Intelligence Service Act brought 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, 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(a) of the Swiss Federal Act on Private International Law of 18 December 1987[14] (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(b) and Paragraph 3 PILA).

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

Privacy and data protection laws and regulations

The Swiss Constitution of 18 April 1999[15] 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.[16] Specific data protection

9 Classified compilation (SR) 780.1.

10 Ordinance on the Supervision of Postal and Telecommunication Services of 18 March 2016, classified compilation (SR) 780.11.

11 Classified compilation (SR) 780.1 and SR 780.11.

12 BBl 2013 2686.

13 Classified compilation (SR) 121 and SR 121.1.

14 Classified compilation (SR) 291, last amended as of 1 April 2017.

15 Classified compilation (SR) 101, last amended as of 12 February 2017.

16 Classified compilation (SR) 235.13, last amended as of 1 November 2016.

issues such as, 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.[17]

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[18]

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'

17 As mentioned in footnote 8, the guidelines are not legally binding, but do set de facto standards.

18 Article 3 DPA.

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.[19]

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

19 Articles 4, 5 and 7 DPA.

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.

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[20] 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;

20 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.

d processes personal data on a professional basis exclusively for publication in the edited section of a periodically published medium;

e 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

f 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).[21] 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.

21 See Article 12 Paragraph 2(c) DPA.

iii Data subject rights

Articles 8–10 DPA define the data subjects' access rights and their scope. Under Article 8 Paragraph 1 DPA, any person may request information from the controller of a data file as to whether data concerning them is being processed. Thereafter, the controller of a data file must notify the data subject of all available data concerning the subject in the data file, including the available information on the source of the data, and must also disclose the purpose of and if applicable the legal basis for the processing as well as the categories of the personal data processed, the other parties involved with the file and the data recipient (Article 8 Paragraph 2(a) and (b) DPA). Where processors are involved, Article 8 Paragraph 4 DPA provides that if the controller of a data file has personal data processed by a third party, the controller remains under an obligation to provide information. The third party is under an obligation to provide information if he or she does not disclose the identity of the controller or if the controller is not domiciled in Switzerland.

Under certain circumstances, the controller of the data file may refuse or limit its disclosure. Indeed, the controller of a data file may refuse, restrict or defer the provision of information where a formal enactment so provides, or this is required to protect the overriding interests of third parties (Article 9 Paragraph 1(a) and (b) DPA), being specified that similar limitations also exist for federal bodies (Article 9 Paragraph 2 DPA). In addition, the private controller of a data file may further refuse, restrict or defer the provision of information where its own overriding interests so require and it does not disclose the personal data to third parties (Article 9 Paragraph 4 DPA). In any case, the controller of a data file must indicate the reason for refusing, restricting or deferring access to information (Article 9 Paragraph 5 DPA), and this must take the form of a substantiated decision (Article 1 Paragraph 4 DPO).

To exercise the access right, the data subject must typically file a written request and provide proof of their identity, though an online request is also possible if the controller of the data file has made this available (Article 1 Paragraphs 1 and 2 DPO). The requested information must be provided within no more than 30 days of receipt of the request. If this is not possible, the controller of the data file must notify the applicant accordingly with an indication of the date by which the information will be provided (Article 1 Paragraph 4 DPO). If a request for information relates to data that is being processed by a third party on behalf of the controller of the data file, the controller must pass the request on to such third party for processing if the controller is not able to provide the information itself (Article 1 Paragraph 6 DPO).

The exercise of the access right is, as a rule, free of charge for the data subject (Article 8 Paragraph 5 DPA). However, the controller of the data file may exceptionally levy from the applicant an appropriate share of the costs up to a maximum of 300 Swiss francs if the provision of information entails an exceptionally large amount of work, or if the applicant has already been provided with the requested information in the 12 months prior to the application and no legitimate interest in the further provision of information can be proven. A legitimate interest exists in particular if the personal data has been modified without notice being given to the data subject (Article 2 DPO).

Pursuant to Article 34 DPA, failure to provide the requested information or the provision of false or incomplete information may lead to a fine as further explained in Section VII.i.

iv Technological innovation and privacy law

In general, the electronic or online context of the data processing does not per se directly impact the applicable legal provisions, so the general provisions remain applicable. That said, certain sector-specific rules may come into play. This is the case for Article 43 of the Telecommunications Act of 30 April 1997 (TCA),[22] which implements 'telecommunications secrecy' and provides that no person who is or has been responsible for providing a telecommunications service may disclose to a third party information relating to subscribers' communications or give anyone else an opportunity to do so. Because the definition of what constitutes a 'telecommunications service' under Swiss law is very broad, in effect encompassing any transfer of data, be it through landlines or via new technologies such as 'over the top' (OTT) delivery, telecommunications secrecy plays an important practical role also for ISPs and web-based service providers.

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.[23]

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 Articles 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.

22 Classified compilation (SR) 784.10, last amended as of 1 September 2017.

23 Commissioner, 'Guide to cloud computing', available at: https://www.edoeb.admin.ch/edoeb/en/home/data-protection/Internet_und_Computer/cloud-computing/guide-to-cloud-computing.html (status 2014; last visited on 19 July 2019).

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 (b) TCA. 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 in effect 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.[24] 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).[25]

v 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

24 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 1 January 2019, classified compilation (SR) 748.941.

25 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 19 July 2019).

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).[26]

Furthermore, Article 26 of Ordinance 3 to the Employment Act[27] 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 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.[28]

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.

26 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.

27 Ordinance 3 to the Employment Act (Healthcare) of 18 August 1993, last amended as of 1 October 2015, classified compilation (SR) 822.113.

28 Commissioner, 'Guide on the processing of personal data in the work area' (status November 2014; https://www.edoeb.admin.ch/edoeb/de/home/dokumentation/taetigkeitsberichte/aeltere-berichte/19--taetigkeitsbericht-2011-2012/buergeranfragen-zur-ueberwachung-am-arbeitsplatz.html, in German; no English version available; last visited on 19 July 2019).

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.[29]

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.

29 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 19 July 2019).

The Commissioner has published a (non-binding) list of countries that provide an adequate data protection level with respect to individuals.[30] 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.[31]

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 (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,[32] 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–

30 See list of countries at https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2017/04/staatenliste.pdf.download.pdf/staatenliste.pdf (in German; no English version available; last visited on 19 July 2019).

31 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.

32 See the standard contractual clauses for the transborder outsourcing of data processing accepted by the Commissioner, available at: https://www.edoeb.admin.ch/edoeb/en/home/data-protection/handel-und-wirtschaft/entreprises/anmeldung-einer-datensammlung/mustervertrag-fuer-das-outsourcing-von-datenbearbeitungen-ins-au.html (status November 2013; last visited on 19 July 2019).

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.[33] 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 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[34] 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(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

33 The dedicated Privacy Shield Framework website sets up this process: www.privacyshield.gov/welcome (last visited on 19 July 2019). It also allows any interested person to consult the list of certified companies: www.privacyshield.gov/list (last visited on 19 July 2019).

34 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).

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 (see Article 11a Paragraph 3 DPA in relation to Article 11a Paragraph 5(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 sovereign judicial 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(c) DPA).[35] 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.[36]

35 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(c) DPA).

36 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

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;
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.[37] 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 recommend putting an end to the data processing activity. 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

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.

37 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.

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 brought before 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;
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).[38]

ii Recent enforcement cases

A recent Swiss Federal Supreme Court case[39] dealt with the admissibility of video surveillance on company premises. According to the Swiss Federal Supreme Court, strict standards apply for video surveillance by criminal prosecution authorities. In particular, any video surveillance by police officers on company premises needs to be ordered by the Public Prosecutor and must be authorised by the competent compulsory measures court to be valid as evidence.

Also relating to 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.[40]

In a leading case dated 18 April 2017, the Swiss Federal Administrative Court dealt with the concept of personality profiles and retrievability of personal data via search engines.[41] 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

38 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.

39 Swiss Federal Supreme Court decision of 20 December 2018, 6B_181/2018.

40 Swiss Federal Supreme Court decision dated 17 January 2015 (BGE 139 II 7).

41 Swiss Federal Administrative Court decision dated 18 April 2017, A-4232/2015.

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.

In a ruling dated 18 October 2016, the European Court of Human Rights (ECHR), 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.

Several recent 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.[42] In three parallel rulings dated 23 August 2016,[43] the Swiss Federal Administrative Court decided on the scope of Article 19 Paragraph 4(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 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)[44] and does not contain information provided by leniency applicants in the sense of Article 49a Paragraph 2 ACart.

Finally, still very relevant and noteworthy is the Swiss Federal Supreme Court's decision of 12 January 2015 in connection with the tax dispute between certain Swiss banks and the

42 Classified compilation (SR) 152.3, last amended as of 19 August 2014.

43 Swiss Federal Administrative Court decisions dated 23 August 2016, A-6334/2014, A-6320/2014 and A-6315/2014.

44 Classified compilation (SR) 251, last amended as of 1 December 2014.

United States. 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.[45]

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 (see above Section III.iii). 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:

a that data processing be stopped;
b that no data be disclosed to third parties;
c that the personal data be corrected or destroyed;
d compensation for moral sufferings; and
e 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 breaches of data protection legislation and personality rights.

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).[46] 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. Nonetheless, Switzerland does not have any 'data territoriality' requirements, meaning that there is no obligation to store personal data in Switzerland.

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

45 Swiss Federal Supreme Court decisions dated 12 January 2015, 4A_406/2014; 4A_408/2014 (BGE 141 III 119).

46 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.

or new obligations for the processing of the personal data may be created that did not exist beforehand.[47] It is therefore strongly recommended that compliance is verified with the DPA before disclosing or transferring any personal data to Switzerland, before starting to process personal 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.[48]

Swiss data security requirements do not impose specific standards. Rather, and in furtherance of a technology-neutral stance, anyone processing personal data must implement technical and organisational measures that are 'adequate' (Article 8 Paragraph 2 DPO) and, in the case of automated processing, 'suitable' for achieving data security goals (Article 9 Paragraph 1 DPO). This wording is generally construed as requiring of anyone processing personal data to implement industry best practices in its cybersecurity processes.

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).[49] 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.[50] 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

47 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).

48 'Guide for technical and organisational measures' (status as of February 2016); https://www.edoeb.admin.ch/dam/edoeb/en/dokumente/2016/02/leitfaden_zu_dentechnischenundorganisatorischenmassnahmendesdate.pdf.download.pdf/guide_for_technicalandorganizationalmeasures.pdf, last visited on 19 July 2019). 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.

49 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=0ahUKEwiZ8vetoovWAhUCshQKHeLuBeMQFggNMAQ&client=internal-uds-cse&usg=AFQjCNH1i9Man6e87Na3Uq4hvV8R2iGy4g, last visited on 19 July 2019).

50 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.

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.[51] 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.

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.[52]

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,[53] 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;

51 More information on CYCO is available at https://www.fedpol.admin.ch/fedpol/en/home/kriminalitaet/cybercrime.html (last visited on 19 July 2019).

52 Classified compilation (SR) 351.1, last amended 1 March 2019.

53 See footnote 6 for links to the draft of the revised DPA.

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.

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, will now unfold in two parts. The first part entered into force in March 2019, while the second part is tentatively expected to enter into force in 2020 or (more likely) 2021 (for further details, see Section II).

Chapter 24

TURKEY

Batu Kınıkoğlu, Selen Zengin and Kaan Can Akdere[1]

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[2] 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, there are certain additional data protection related provisions provided under the Banking Law for financial services and these are enforced by the Turkish banking authority, the Banking Regulation and Supervision Agency.

Because Turkey is currently not an EU country, in principle, EU's General Data Protection Regulation[3] (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 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.

---

1 Batu Kınıkoğlu is a partner, and Selen Zengin and Kaan Can Akdere are attorneys at BTS&Partners.

2 Published in the Official Gazette No. 17844 and dated 20 October 1982. Available in English: https://global.tbmm.gov.tr/docs/constitution_en.pdf.

3 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal L 119, 4 May 2016.

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. However, recently enacted legislation demonstrates the sensitivity that is being shown by the government regarding cybersecurity, which we expect to become an even more important topic for Turkey in the near future.

II THE YEAR IN REVIEW

Data protection has been an active legal area since the enactment of the DP Law. From the Board's perspective, 2019 has been the year of enforcement decisions and guidance for data controllers. The Board has been continuously publishing enforcement decisions concerning unlawful collection and processing of personal data by both private companies and government entities alike. And for the first time since its establishment, Board decisions are more detailed and the identities of the relevant data controllers and the amounts of the fines issued are disclosed. This transparency approach adopted by the Board and concerns regarding reputational risks have forced the data controllers processing personal data in Turkey to be more diligent about being compliant with the DP Law.

The most important decisions published by the Board since November 2018 are those regarding unsolicited commercial communications and data breach notifications. According to the decision published on 1 November 2018, the Board has received numerous complaints from data subjects concerning the fact that their communications addresses are being used to send unsolicited marketing calls and messages without their consent. In its decision, the Board explicitly stated that prior consent of the data subject is required to process personal communication data for the purpose of sending commercial messages. In its decision of 15 February 2019, the Board announced the principles and procedures to be followed when submitting personal data breach notifications to the Board in accordance with Article 12 of the DP Law. According to the decision, data controllers are expected to notify the Board as soon as possible and no later than 72 hours[4] after they become aware of the breach; the notifications are to be made via a template notification form and the data controllers are expected to prepare a 'data breach response plan' that will cover issues such as steps to be followed within the organisation to handle breaches and responsibilities regarding such incidents.

Based on the enforcement decisions published by the Board, the heaviest fines were issued in response to data breaches of an international nature that involved the personal data of Turkish citizens. For example, the Board issued its highest fines in its decisions concerning data breaches that involved global companies such as Marriott International Inc,[5] Cathay Pacific Airway Limited[6] and Facebook,[7] with fines of 1.45 million, 550,000 and 1.65 million Turkish lira respectively.

4 Notably, the Board have made a reference to the 72 hour period provided under the GDPR as a basis for this rule.

5 https://www.kvkk.gov.tr/Icerik/5479/2019-143.

6 https://www.kvkk.gov.tr/Icerik/5480/2019-144.

7 https://www.kvkk.gov.tr/Icerik/5481/2019-104.

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 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[8]

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[9]

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.

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.

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.

ii 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:

a conforming to the law and good faith principles;
b being accurate and, if necessary, up to date;
c processing for specified, explicit and legitimate purposes;
d processing that is relevant, limited and proportionate to the stated purposes; and
e 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:

a if none of the following conditions can be met, explicit consent[10] of the data subject,
b if processing is expressly permitted by any law;
c 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;
d 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;
e if processing is necessary for compliance with a legal obligation which the controller is subject to;
f if the relevant information is publicised by the data subject herself or himself;
g if processing is necessary for the institution, usage, or protection of a right; and
h 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.

10 '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.

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:

a the identity of the data controller and, if any, its representative;
b the purposes for which personal data will be processed;
c the persons to whom processed personal data might be transferred and the purposes for the same;
d the method and legal cause of collection of personal data; and
e the rights set forth under Article 11 of the DP Law.

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. The Registry is currently active and accepting registrations.

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. The deadline for registering is 30 September 2019 for local and foreign private data controllers.

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 Board[11] 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[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:

a learn whether their personal data have been processed;
b request information as to processing if their data have been processed;
c learn the purpose of processing of their personal data and whether data are used in accordance with their purpose;
d learn the third parties those which their personal data have been transferred;
e request rectification in case personal data are processed incompletely or inaccurately;
f request deletion or destruction of their personal data within the framework of the conditions set forth under Article 7;
g request notification of the operations made as per indents (e) and (f) to third parties to whom personal data have been transferred;
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; and
i request compensation for the damages in case the they incur damages owing to unlawful processing of their personal data.

11 Guidebook on Personal Data Security (Technical and Organisational Security Measures): https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/7512d0d4-f345-41cb-bc5b-8d5cf125e3a1.pdf.

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.

vii Specific regulatory areas

Electronic marketing

In addition to the general provisions of the DP Law, electronic marketing communications are regulated under a separate regulation, the Regulation on Commercial Communications and Electronic Commercial Communications.[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 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 Law[15] about banking secrecy and 'customer secrets', and the Regulation on Personal Health Data that mainly concerns the healthcare sector.[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.

13 Published in the Official Gazette No. 29417 and dated 15 July 2015.

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. 30808 and dated 21 June 2019.

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.

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 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 August 2019, the Board has not yet published the list of 'safe countries'.

17 Council of State, 11th Chamber, Decision No. 2017/4906 dated 13 June 2017.

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.

V COMPANY POLICIES AND PRACTICES

i 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.

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 during registration, 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 multiple principle decisions to date including some concerning phonebook applications, the implementation of privacy measures on counters and booths, and data breaches caused by data controllers' personnel, data breach notifications and unsolicited marketing communications. 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 numerous enforcement decisions on its website.[21] Previously, the summaries did not include the identities of the data controllers or the amount of fines; however, the Board has been more transparent in its more recent decisions and has published names and amounts. The majority of fines were due to a breach of data security obligations, even when the breach was caused by a violation 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 (and has been demonstrated by the enforcement decisions concerning foreign data controllers).[22] Consequently, foreign data controllers are expected to comply with the obligations listed in the DP Law if they carry out personal data processing activities that affect individuals located in Turkey.

The notable obligations foreign data controllers are required to comply with 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):

a 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

b collecting and forwarding the data subject applications to the data controller;

21 Personal Data Protection Board, Decision Summaries: https://www.kvkk.gov.tr/Icerik/5406/Kurul-Karar-Ozetleri.

c transmit the responses given by data controllers in relation to data subject applications; and

d 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. However, the recently enacted Circular Note on Information and Communication Security Measures numbered 2019/12[23] (the Circular) establishes extensive cybersecurity-related obligations that are mainly applicable to public authorities and institutions. The most notable measures contained within the Circular are (1) significantly limiting the use of cloud systems; and (2) seriously restricting social media use in the public sector.

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)[24] and entities from sectors such as insurance,[25] banking[26] and payment services[27] 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.[28] 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 Board has clarified that data controllers must notify the Board within 72 hours of becoming aware of the breach, by making use of the data breach notification form published by the Board.[29]

23 Published in the Official Gazette No. 30823 and dated 6 July 2019.

24 See Communiqué on Information System Management, published in the Official Gazette No. 30292 and dated 5 January 2018.

25 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.

26 See Regulation on Internal Systems of Banks and Evaluation Process for Efficiency of Internal Capital, published in the Official Gazette No. 29057 and dated 11 July 2014.

27 See Regulation on the Activities of the Payment and Security Settlement Systems, published in the Official Gazette No. 29044 and dated 28 June 2014.

28 CERT Website available in English: https://www.usom.gov.tr/.

29 See the data breach notification form published by the Board, available in Turkish at: https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/617f166c-24e1-42b5-a9cb-d756d6443af9.pdf.

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 three 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.

Chapter 25

UNITED KINGDOM

William RM Long, Géraldine Scali and Francesca Blythe[1]

I OVERVIEW

Like other countries in Europe, the United Kingdom (UK) passed legislation designed to supplement the data protection requirements of the EU General Data Protection Regulation (GDPR),[2] which came into force on 25 May 2018, repealing the EU Data Protection Directive 95/46/EC (the Data Protection Directive)[3] 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, repealed the UK Data Protection Act 1998 (DPA 1998), introduced 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[4] 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

The ICO has published a variety of guidance addressing compliance with the GDPR[5] and the DPA 2018 including in relation to the impact of Brexit, which will be highly significant from a data protection perspective and further details are provided in Section XII.

Following the entry into force of the GDPR, the ICO has reported having received large volumes of personal data breach notifications and complaints from individuals. As a result, the resources of the ICO are reportedly at full capacity, which has resulted (until recently) in delays in handling reported breaches. However, we do expect further acceleration

1 William RM Long is a partner, Géraldine Scali is a counsel and Francesca Blythe is a senior associate at Sidley Austin LLP.

2 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

3 European Parliament and Council Directive 95/46/EC 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.

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.

5 ICO, Guide to the General Data Protection Regulation (GDPR) accessible at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/.

in enforcement action under the GDPR in the coming months and this is demonstrated by the ICO providing in July 2019 notices of its intention to fine two companies for cyber breaches and further details are provided in Section IX below.

Consumer awareness in relation to data protection issues also appears to have dramatically increased; in particular, the fact that consumers can exercise their rights under the GDPR, such as the right of erasure and right of access to personal data. This is illustrated by the fact that the ICO received 6,281 complaints between 25 May to 3 July 2018 – a 160 per cent rise compared with the same period in 2017. Despite this growth in consumer awareness, privacy litigation has been limited to date. However, attempts at collective redress are becoming more frequent and further details are provided in Section IX below.

III REGULATORY FRAMEWORK

i Privacy and data protection laws and regulations

Data protection in the UK is 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 implement Directive 2002/58/EC[6] (as amended by Directive 2009/136/EC) (the ePrivacy Directive). The ICO has 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.[7] 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 2021 at the earliest. As a result, it remains to be seen whether the UK will in any case choose to implement the ePrivacy Regulation into domestic law post-Brexit.

The key changes in the proposed ePrivacy Regulation will:

a require a clear affirmative action to consent to cookies;

b attempt to encourage the shifting of the burden of obtaining consent for the use of cookies to website browsers; and

6 Directive 2002/58/EC of the European Parliament and Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

7 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).

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

The terms used in the DPA 2018 have the same meaning as they have in the GDPR.[8] The key terms are:

a 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 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 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, 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 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;

c ruling on complaints; and

d taking regulatory actions.

8 Section 5 of the DPA 2018.

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, 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 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 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.[9] In particular, the ICO has also published detailed guidance on legitimate interests as a legal basis together with a legitimate interest assessment template[10] that covers three tests controllers should conduct as part of any legitimate interest 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.

The ICO's guidance on the GDPR also contains a section on consent, which makes reference to the GDPR's high standard for valid consent i.e., that consent be unambiguous, involve a clear affirmative action and provide 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 demonstrate 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 additional conditions being fulfilled.[11]

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 special categories of personal data, controllers must identify a legal basis under Article 6 of the GDPR and a condition under Article 9 of the GDPR. The DPA 2018 introduces additional conditions for processing special categories of 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.;
d preventing fraud;
e insurance; and
f occupational pensions.

9 ICO, Guide to the General Data Protection Regulation (GDPR)/ Lawful basis for processing- accessible at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/.

10 ICO, Sample LIA template.

11 Articles 9 and 10 of the GDPR, Sections 10 and 11 and Schedule 1 of the DPA 2018.

Where processing special categories of 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 special categories 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 EU 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:

a consent;
b protecting data subjects vital interests;
c processing by not-for-profit bodies;
d personal data in the public domain;
e legal claims;
f judicial acts;
g administration of accounts used in commission of indecency offences involving children; and
h 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' as explained in Section IV(iii) above.

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:

a it is likely to cause substantial damage or distress to an individual; or
b 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:

a 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[12];
b 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.[13]

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.[14]

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), involve[15]:

a 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
b 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.

The DPO must be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices.[16] 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, which includes:

a the contact details of the DPO;
b the registration number of the controller or processor; and
c 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:

a 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;

b providing advice on the carrying out of a data protection impact assessment (see below) and monitoring compliance;

c cooperating with the ICO;

d acting as the contact point for the ICO on issues relating to processing of personal data;

e monitoring compliance with the policies of the controller in relation to the protection of personal data; and

f 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[17] (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 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.

Article 30 of the GDPR requires controllers to also keep a record of their processing activities. Processors are also under an obligation to keep a record of processing activities carried out on behalf of 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.[18]

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,[19] in particular on the data subject's right to be informed, suggests the information notice can take many forms, including:

a a layered approach: this will usually be a short notice containing key privacy information, with additional layers of more detailed information;

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;

17 Data Protection (Charges and Information) Regulations 2018/480.

18 Article 30 of the GDPR.

19 ICO, Guide to the General Data Protection Regulation (GDPR)/ Individual Rights/ Right to be Informed-accessible at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/.

c just-in-time notices: relevant and focused privacy notices delivered at the time the personal data is collected;
d icons: small, meaningful symbols that highlight the existence of data processing; and
e mobile and smart device functionalities: these include pop-ups, voice alerts and mobile device gestures.

ix Data protection impact assessments (DPIA)

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:

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
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:

a a general description of the envisaged processing operations;
b an assessment of the risks to the rights and freedoms of data subjects;
c the measures envisaged to address those risks; and
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.[20]

x 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,[21] 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.

20 ICO, Guide to the General Data Protection Regulation (GDPR)/ Accountability and Governance- accessible at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/.

21 ICO, Guide to the General Data Protection Regulation (GDPR)/Principles/Purpose limitation, accessible at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/.

xi 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,[22] 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.[23]

xii 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[24] 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.

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.[25]

22 ICO, Guide to the General Data Protection Regulation (GDPR)/Principles/Data minimisation, accessible at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/.

23 ibid.

24 ICO, Guide to the General Data Protection Regulation (GDPR)/Principles/Accuracy, accessible at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/.

25 ICO, Guide to the General Data Protection Regulation (GDPR)/Principles/Storage limitation, accessible at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/.

The ICO, in its published guidance on the GDPR, contains guidance on storage limitation, recommending that controllers erase or anonymise personal data[26] where they 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 guidance[27] 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.

In its GDPR guidance on individuals' rights the ICO states that if a valid erasure request is received and no exemption applies then a controller will have to take steps to ensure erasure from backup systems as well as live systems. However, the ICO acknowledges that the data will remain within the backup environment for a certain period of time until it is overwritten. According to the ICO, the key issue is to 'put the backup data "beyond use", even if it cannot be immediately overwritten'. Provided that the controller does not use the data within the backup for any other purpose, 'it may be unlikely that the retention of personal data within the backup would pose a significant risk, although this will be context specific'.

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 processor to process personal data on its behalf, the controller must ensure that it has entered into a written contract that obliges the 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,[28] that 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 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.[29]

26 ICO, Guide to the General Data Protection Regulation (GDPR)/Principles/Storage limitation, accessible at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/.

27 ibid.

28 ICO, Guide to the General Data Protection Regulation (GDPR)/Security, accessible at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/.

29 ibid.

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.[30]

The ICO considers encryption to be an appropriate technical measure owing to its widespread availability and relatively low cost of implementation.[31] 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: accountability

The data protection principle of accountability under Article 5.2 of the GDPR is prevalent throughout the GDPR and requires controllers to not only comply with the GDPR but to demonstrate their 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 guidance[32] 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 having written contracts in place with vendors processing personal data, that comply with Article 28 of the GDPR;
d maintaining records of processing activities;
e recording and, where necessary, reporting personal data breaches;
f carrying out DPIAs for uses of personal data likely to result in a high risk to the data subject's interests; and
g adhering to relevant codes of conduct and sign up to certification schemes.

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.[33] The framework could include:

a robust programme controls informed by the GDPR requirements;
b appropriate reporting structures; and
c assessment and evaluation procedures.

In July 2019, the ICO published a draft statutory code of practice on data sharing between controllers. The draft code outlines how organisations should engage in data-sharing activities (including the requirement to have in place a data sharing agreement to help demonstrate accountability under the GDPR). The draft code also guidance on risk management processes, best practices and misconceptions about data sharing.

30 ibid.
31 ibid.
32 ICO, Guide to the General Data Protection Regulation (GDPR)/Accountability and governance, accessible at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/.
33 ibid.

V TECHNOLOGICAL INNOVATION AND PRIVACY LAW

i 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[34] that recommended organisations using anonymisation have in place an effective and comprehensive governance structure that should include:

a a senior information risk owner with the technical and legal understanding to manage the process;

b staff trained to have a clear understanding of anonymisation techniques, the risks involved and the means to mitigate them;

c procedures for identifying cases where anonymisation may be problematic or difficult to achieve in practice;

d knowledge management regarding any new guidance or case law that clarifies the legal framework surrounding anonymisation;

e a joint approach with other organisations in the same sector or those doing similar work;

f use of a privacy impact assessment;

g 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;

h a review of the consequences of the anonymisation programme; and

i 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 analytics. The ICO issued guidance in July 2014 and revised it in August 2017[35] considering the data protection issues raised by big data. The ICO suggested how controllers can comply with the DPA 2018 and the GDPR while using big data, covering a broad range of topics including anonymisation, DPIAs, repurposing data, data minimisation, transparency and subject access. The guidance included three questions on which the ICO invited feedback. A summary of feedback was published in April 2015.[36]

34 In November 2012, the ICO published a code of practice on managing data protection risks related to anonymisation. This code provides a framework for organisations considering using anonymisation and explains what it expects from organisations using such processes.

35 ICO, Guidelines on Big Data and Data Protection, 28 July 2014 and revised 18 August 2017.

36 ICO, Summary of Feedback on Big Data and Data Protection and ICO Response, 10 April 2015.

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.[37] 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)[38] 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 organisations 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.

iv Cloud computing

The ICO, like many other data protection authorities in the EU, published guidance on cloud computing, in 2012.[39]

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.[40]

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.

37 FCA, FS16/5, Call for Inputs on Big Data in retail general insurance.
38 ICO, Guidelines on Bring Your Own Device (BYOD), 2013.
39 ICO, Guidance on the Use of Cloud Computing, 2012.
40 See the European Union Overview chapter for more details on cloud computing.

v Cookies and similar technologies

Article 5(3) of the ePrivacy Directive 2002/58/EC – implemented in the UK through the PECR – requires consent for the use of cookies and similar technologies. As a result, organisations have an obligation to obtain the consent of website users to place cookies or similar technologies on their computers and mobile devices.[41] 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.

In July 2019, the ICO published new guidance on the use of cookies and similar technologies. In the new guidance the ICO formally recognises the stricter standards of consent and transparency now in force under the GDPR. In particular, the new guidance states that:

a consent for non-essential cookies must comply with GDPR standards, which means it must involve: (1) a clear positive action (continuing to browse the website is not sufficient) and not implied consent; (2) granularity (the ability to consent to cookies used for some purposes, but not others); and (3) no pre-ticked boxes or sliders set to 'on' (i.e., the default option for non-essential cookies must be off);

b the legitimate interest legal ground cannot be used as an alternative for consent to place non-essential cookies on a website;

c blanket cookie walls to restrict access to websites until a user consents to the use of cookies are unlikely to represent valid consent. The guidance confirms that statements such as 'by continuing to use this website you are agreeing to cookies' is not considered valid consent under the higher GDPR standard;

d information provided on cookies must align with the GDPR standards for transparency; and

e if an organisation's use of cookies changes significantly, users will need to be made aware of these changes to allow them to make an informed choice about the new activity.

To help address the above, the ICO recommends that organisations conduct a 'cookie audit' which will: (1) confirm the purpose(s) of each cookie; (2) confirm the type of cookie (session or persistent); (3) distinguish between those that are strictly necessary and non-essential; (4) document the findings; and (5) consider follow-up actions while building in an appropriate review period. The ICO views this as an opportunity for organisations to 'clean up' existing web pages and stop using unnecessary cookies, particularly if the website has evolved since an initial assessment was undertaken.

The new guidance confirms that enforcement action will vary, as expected, depending on the level of privacy intrusion and risk of harm posed by cookies and related technologies. The current enforcement regime for PECR remains as was in effect under the DPA 1998 (except where personal data is processed, in which case the GDPR enforcement penalties

41 PECR Regulation 6.

will apply). However, it is expected that this will be brought into line with the GDPR with the introduction of the ePrivacy Regulation, which will replace the ePrivacy Directive when finalised.[42]

VI SPECIFIC REGULATORY AREAS

i Minors

In April 2019, the ICO published its draft Age Appropriate Design Code setting out guidance for online services likely to be accessed and used by children under 18. The draft Code applies to information society services (which in practice would include all online services) and sets out 16 standards of age-appropriate design for information society services. The ICO intends that the draft Code will be finalised by the end of 2019.

ii 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 UK data protection laws and to adopt good practices.[43]

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.

iii Employee monitoring[44]

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 EDPB's Guidance on Data Protection Impact Assessments[45] provides examples of when a DPIA should be carried out and an employee monitoring programme is identified as an example of when a DPIA should

42 See the European Union Overview chapter for more details on the proposed ePrivacy Regulation.

43 ICO, The Employment Practices Code: Supplementary Guidance, November 2011.

44 ibid.

45 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.

be carried out. Likewise, the ICO in its Guidance on DPIAs states that a controller should think carefully about doing a DPIA for any processing that inter alia involves monitoring, sensitive data or vulnerable individuals (e.g., employees).

Organisations should carry out a DPIA 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.

On 8 June 2017, the former Article 29 Working Party adopted an opinion on data processing at work that also addressed employee monitoring.[46] This opinion is unlikely to fundamentally change the ICO's approach to employee monitoring in the UK. 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.

iv 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,[47] 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 UK will have to comply with the data-protection principles under the DPA 2018 and the GDPR.[48]

v Electronic marketing[49]

Under PECR, unsolicited electronic communications to individuals should only be sent with the recipient's consent.[50] 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

46 WP 249: Opinion 2/2017 on data processing at work, adopted 8 June 2017.

47 ICO, 'Disclosures from whistleblowers', 2 June 2017.

48 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.

49 ICO, Guide to the Privacy and Electronic Communications Regulations, 2013, and Direct Marketing Guidance, V.2.2.

50 PECR Regulation 22(2).

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.[51]

Senders of electronic marketing messages must provide the recipients with the sender's name and a valid contact address.[52]

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 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.[53] The ICO launched a consultation phase on a Direct Marketing Code of Practice, which closed in December 2018 and 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.[54] 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 UK if it takes effect before the UK exits the European Union on 31 October 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.[55]

vi 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.[56]

Failure to comply with these security requirements may lead to the imposition of significant financial penalties by the FCA.

51 Guide to PECR/ Electronic and telephone marketing/ electronic mail marketing- accessible at https://ico.org.uk/for-organisations/guide-to-pecr/electronic-and-telephone-marketing/electronic-mail-marketing/.

52 PECR Regulation 23.

53 ICO, Direct Marketing Guidance, V.2.2.

54 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/.

55 See the European Union overview chapter for more details on the proposed ePrivacy Regulation.

56 SYSC 3.

VII INTERNATIONAL TRANSFERS

The GDPR prohibits the transfer of personal data outside of the EEA to third countries (non-EEA Member State) unless:

a the recipient country is considered to offer an adequate level of data protection; or

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

c a derogation from the prohibition applies (such as the data subject has explicitly consented to the transfer).

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 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:

a 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;

b where the controller has assessed all the circumstances surrounding the data transfer and has, as a result, implemented suitable data protection safeguards; and

c 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:

a to protect the vital interests of the data subject or another person;

b to safeguard the legitimate interests of the data subject;

c for the protection of an immediate and serious threat to the public security of a Member State or a third country;

d 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

e 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.

Brexit will have fundamental implications for data protection and the ongoing flow of personal data from the EU to the UK, and vice versa. However, as with many other issues, the precise implications will depend on whether a deal is reached between the EU and the UK. In particular, if the UK leaves the EU without a deal, the UK will be considered a third country from 31 October 2019, and transfers from the EU to the UK will be restricted. In this scenario, companies will have to put in place a valid data transfer solution to legitimise their transfers of personal data from the EU to the UK (e.g., EU standard contractual clauses). However, in the event a deal is reached on the Withdrawal Agreement, Article 127 of the Withdrawal Agreement provides that EU law (i.e., the GDPR) will be applicable in the UK through the 'Transition Period' (currently until 31 December 2020) which has been interpreted to mean that during the Transition Period, transfers of personal data from the EU to the UK will not be considered transfers to a third country. In short, during the Transition Period the UK will still be treated as an EU Member State. As such, during the Transition Period there will be no need for a data transfer solution for transfers of personal data from the EU to the UK.

VIII DISCOVERY AND DISCLOSURE

The ICO has not published any specific guidance on this topic.[57] 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.

57 The Article 29 Working Party has, however, published a working document on this topic. See the European Union Overview chapter for more details.

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, 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 DPA 1998, continue to have effect under the DPA 2018.

In a speech at the Data Protection Practitioners' Conference on 9 April 2018, the Information Commissioner, Elizabeth Dunham, stated that 'enforcement is a last resort' and that '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

Until July 2019, GDPR-related enforcement action by the ICO was limited. The only exceptions to this was the enforcement notice issued to a Canadian data analytics firm in October 2018 in relation to its political campaign behavioural advertising techniques and the issuance of more than 100 fines to companies across a range of sectors that failed to pay the data protection registration fee to the ICO.

However, on 8 July 2019, the ICO issued a notice of its intention to fine British Airways (BA) £183.39 million for infringements of the GDPR. The proposed fine relates to a cyber incident that BA notified to the ICO (as BA's lead data protection authority) in September 2018. The incident involved the theft from the BA website and mobile app of personal data relating to customers over a two-week period.

Then on 9 July 2019, the ICO issued another statement of its intention to fine Marriott International, Inc over £99 million in relation to a security incident affecting the Starwood reservation database that Marriott had acquired in 2016 and discovered in November 2018. The statement came in response to Marriott's filing with the US Securities and Exchange Commission that the ICO intended to fine it for breaches of the GDPR. The UK Information Commissioner confirmed in a statement that 'organisations must be accountable for the personal data they hold and this includes carrying out proper due diligence when making a corporate acquisition, and putting in place proper accountability measures to assess not only what personal data has been acquired, but how it is protected.'

Both BA and Marriott now have an opportunity to make representations to the ICO as to the proposed findings and sanctions.

iii Private enforcement

Under the GDPR, data subjects are able to claim for 'material or non-material damage' as a result of a breach of the GDPR. In addition, not-for-profit organisations have the right to lodge a complaint on behalf of the data subject. For example, BA has been threatened with a £500 million class action lawsuit in a UK court for non-material damage caused by the personal data breach mentioned above. BA had already pledged to cover any losses suffered by its customers, but a law firm acting for some of the affected individuals has taken the position that under the GDPR, the individuals have a right to further compensation of £1,250 each.

A recent case in the UK relates to a former employee who copied payroll data of 100,000 employees onto an external drive and subsequently posted the data on a file sharing website. The individual was jailed for eight years under the UK's Computer Misuse Act. The employer was found vicariously liable to approximately 5,000 employees who joined group litigation for breach of confidence and UK data protection laws because it was held that there was a sufficient connection between the employer having authorised the tasks of the former employee (i.e., he was entrusted with the payroll data) and the wrongful acts committed by him.

X CONSIDERATIONS FOR FOREIGN ORGANISATIONS

The DPA 2018 applies to a controller established in the UK and processing personal data in the context of that establishment, regardless of whether the processing takes place in the UK. 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. Controllers not established in the UK 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

Investigatory Powers Act 2016 (the Investigatory Powers Act)

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.[58] 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 had six months to introduce changes to the IPA to make it compatible with UK law. On 31 October 2018 the Data Retention and Acquisition Regulations 2018 came into force to address the UK High Court's ruling.

58 Case C-698/15 *Secretary of State for the Home Department v. Tom Watson, Peter Brice and Geoffrey Lewis*.

The Regulation of Investigatory Powers Act 2000 (RIPA)

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 UK 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 UK'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 impose 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.

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.

Data breaches

Under the GDPR 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.[59] 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.[60] Under the GDPR, processors also have an obligation to notify the controller of personal data breaches without undue delay after becoming aware of a personal data breach.[61]

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.[62] The ICO have stated the 72-hour deadline to report a personal data breach includes evenings, weekends and bank holidays[63] 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:

a the number of data subjects affected by the personal data breach;

b the type of personal data that has been affected;

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

59 Article 33(1) of the GDPR.

60 Article 34 of the Regulation.

61 Article 33(2) of the Regulation.

62 ICO, Guidance on Notification of Data Security Breaches to the Information Commissioner's Office, 27 July 2012.

63 ICO, Personal Data Breach Reporting Webinar, 19 July 2018.

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,[64] 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[65] and the Notification Regulation,[66] 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.[67] The ICO has published guidance on this specific obligation to report breaches.[68]

XII OUTLOOK

The UK is due to depart the European Union on 31 October 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 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.

More generally, it is expected the ICO will continue to publish guidance on the GDPR and DPA 2018 during 2019 and beyond. We also expect further acceleration in enforcement action from the ICO in the coming months as well as a steep increase in consumers exercising their privacy rights and a growth in privacy litigation.

64 ibid.

65 PECR Regulation 5A(2).

66 Commission Regulation No. 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications (the Notification Regulation), which entered into force on 25 August 2013.

67 Article 2 of the Notification Regulation. The content of the notification is detailed in Annex 1 to the Notification Regulation.

68 ICO, Guidance on Notification of PECR Security Breaches, 26 September 2013.

Chapter 26

UNITED STATES

Alan Charles Raul, Christopher C Fonzone and Snezhana Stadnik Tapia[1]

I OVERVIEW – THE 'CHANGING ZEITGEIST'

Nearly 130 years ago, two American lawyers, Samuel Warren and Louis Brandeis – the latter of whom would eventually become a Supreme Court Justice – wrote an article in the *Harvard Law Review* expressing their concern that technological advances like 'instantaneous photographs' and the 'newspaper enterprise' were threatening to 'make good the prediction that "what is whispered in the close shall be proclaimed from the house-tops"'.[2] To address this trend, Warren and Brandeis argued that courts should recognise a common law tort based on violations of an individual's 'right to privacy'.[3] US courts eventually accepted the invitation, and it is easy to consider Warren and Brandeis's article as the starting point of modern privacy discourse.

It is also easy to consider the article as the starting point of the United States' long history of privacy leadership. From the US Supreme Court recognising that the US Constitution grants a right to privacy against certain forms of government intrusion to the US Congress's enacting the Privacy Act to address potential risks created by government databases to US states adopting laws imposing data breach notification and information security requirements on private entities, the United States has long innovated in the face of technological and societal change.

---

1 Alan Charles Raul and Christopher C Fonzone are partners, and Snezhana Stadnik Tapia is an associate, at Sidley Austin LLP. The authors wish to thank Vivek K Mohan, 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.

2 Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 *Harv. L. Rev.* 193 (1890). The piece by Warren and Brandeis is the second most-cited law review article of all time. See Fred R. Shapiro & Michelle Pearse, The Most-Cited Law Review Articles of All Time, 110 *Mich. L. Rev.* 1483, 1489 (2012) (noting that the most cited is R.H. Coase's 'The Problem of Social Cost', which famously introduced 'The Coase Theorem'). It has also created an arms race among legal scholars to come up with new superlatives to describe it: 'monumental', Gordon, Right of Property in Name, Likeness, Personality and History, 55 *Nw. U.L. Rev.* 553, 553 (1960); an article of 'prestige and enormous influence', Robert C. Post, Rereading Warren and Brandeis: Privacy, Property, and Appropriation, 41 Case W. *Res. L. Rev.* 647, 647 (1991); the 'most influential law review article of all', Harry Kalven, Jr., Privacy in Tort Law – Were Warren and Brandeis Wrong?, 31 *Law & Contemp. Probs.* 326, 327 (1966); etc.; etc.

3 Warren & Brandeis, *supra* note 2, at 213.

In recent years, however, privacy commentators have painted the United States in a different light. Over the last generation, the United States has balanced its commitment to privacy with its leadership role in developing the technologies that have driven the information age. This balance has produced a flexible and non-prescriptive regulatory approach focused on post hoc government enforcement (largely by the Federal Trade Commission) and privacy litigation rather than detailed prohibitions and rules, sector-specific privacy legislation focused on sensitive categories of information, and laws that seek to preserve an internet 'unfettered by Federal or State regulation'. The new technologies that have changed the day-to-day lives of billions of people and the replication of US privacy innovations around the globe have – at least to US regulators – long indicated the wisdom of this approach.

But there is now a growing perception that other jurisdictions have seized the privacy leadership mantle by adopting more comprehensive regulatory frameworks, exemplified by the European Union's General Data Protection Regulation. And a series of high-profile data breaches in both the public and private sectors and concerns about misinformation and the misuse of personal information have created a 'crisis of new technologies' or 'techlash' that is shifting popular views about privacy in the United States. Once again, it seems, the United States will be undergoing a period of intense privacy innovation in response to a new technological world.

In short, the US privacy zeitgeist is shifting – and this chapter, while not providing a comprehensive overview of the rich US privacy and cybersecurity landscape, will attempt to show how that is the case. The chapter will begin with an overview of the existing US regulatory and enforcement framework – which exemplifies the balance between privacy protection and innovation described above. The chapter will then describe, with a focus on the concrete developments over the past year, the significant shift in US privacy regulation that appears to be underway.

How all three branches of the federal US government are actively taking steps to confront the privacy and cybersecurity questions of the day – for example, how the Congress, for the first time in a generation, is seriously considering comprehensive federal privacy legislation; how the Supreme Court is extending constitutional rights to digital data held by third parties; and how the executive branch is taking numerous steps to better secure our networks and ensure companies are respecting their users' privacy.

How the real action may not be in Washington DC, but rather in the 50 US states – as California has recently enacted a far-reaching comprehensive privacy bill called 'California's GDPR', and numerous other states either have enacted or are considering substantial new privacy legislation.

And how, not to be outdone, companies are also increasingly recognising that they have to establish 'digital governance' at the board or C-suite level to address strategy and oversight for privacy, data protection, cybersecurity and disruptive technologies.

The chapter concludes by detailing some considerations for foreign organisations that must engage with the US privacy regime and some thoughts on how that regime may continue to evolve going forward.

II THE US REGULATORY FRAMEWORK, INCLUDING PUBLIC AND PRIVATE ENFORCEMENT

As noted above, businesses in the United States are subject to a web of privacy laws and regulations at the federal and state level. Privacy and information security laws typically focus on the types of citizen and consumer data that are most sensitive and at risk, although if one of the sector-specific federal laws does not cover a particular category of data or information practice, then the Federal Trade Commission (FTC) Act, and each state's 'little FTC Act' analogue, comes into play. As laid out below, these general consumer protection statutes broadly, flexibly, and comprehensively proscribe unfair or deceptive acts or practices. Federal and state authorities, as well as private parties through litigation, actively enforce many of these laws, and companies also, in the shadow of this enforcement, take steps to regulate themselves. In short, even in the absence of a comprehensive federal privacy law, there are no substantial lacunae in the regulation of commercial data privacy in the United States. Indeed, in a sense, the United States has not one, but many, de facto privacy regulators overseeing companies' information privacy practices, with the major sources of privacy and information security law and standards in the US these regulators enforce – federal, state, private litigation, and industry self-regulation – briefly outlined below.

i Privacy and data protection legislation and standards – federal law (including general obligations for data handlers and data subject rights)

General consumer privacy enforcement agency – The FTC

Although there is no single omnibus federal privacy or cybersecurity law nor designated central data protection authority, the FTC comes closest to assuming that role for consumer privacy in the US.[4] The statute establishing the FTC, the FTC Act, grants it jurisdiction over essentially all business conduct in the country affecting interstate (or international) commerce and individual consumers.[5] And while the Act does not expressly address privacy or information security, the FTC has interpreted the Act as giving it authority to regulate information privacy, data security, online advertising, behavioural tracking and other data-intensive, commercial activities – and accordingly to play a leading role in laying out general privacy principles for the modern economy.

The FTC has rooted its privacy and information security authority in Section 5 of the FTC Act, which charges the Commission with prohibiting 'unfair or deceptive acts or practices in or affecting commerce'.[6] An act or practice is deceptive under Section 5 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'. The FTC has taken action against companies for deception when companies have made promises, such as those relating to the security procedures purportedly in place, and then not honoured or implemented them in practice. 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 thus understands unfairness to encompass unexpected information practices, such as inadequate disclosure or actions that a consumer would find 'surprising' in the relevant context.

A few examples of what the FTC believes constitutes unfair or deceptive behaviour follow. First, the FTC takes the position that, among other things, 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. To this end, the FTC brought an enforcement action in 2009 against Sears for allegedly failing to disclose adequately 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 behaviour that occurs on [. . .] computers'. The FTC thus required Sears to disclose prominently any data practices that would have significant unexpected implications in a separate screen outside any user agreement, privacy policy or terms of use.[7]

Second, the FTC also takes the position that Section 5 generally prohibits 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.[8]

Finally, 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.[9]

The FTC has not, however, indicated that opt-in consent for the use of non-sensitive information is necessary in behavioural advertising.

In terms of enforcement, the FTC has frequently brought successful actions under Section 5 against companies that did not 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. Although various forms of relief (such as injunctions and damages) for privacy-related wrongs are available, the FTC has frequently resorted to issuing consent decrees. Such decrees generally provide for ongoing monitoring by the FTC, prohibit further violations of the law, and subject businesses to substantial financial penalties for consent decree violations. These enforcement actions have been characterised as shaping a common law of privacy that guides companies' privacy practices.[10]

Cybersecurity and data breaches – federal law

Cybersecurity has been the focus of intense attention in the United States in recent years, and the legal landscape is dynamic and rapidly evolving. Nonetheless, at the time of writing, there is still no general law establishing federal data protection standards, and the FTC's Section 5 authority, as laid out above, remains the closest thing to a general national-level cybersecurity regulator.

---

7 Complaint, *In re Sears Holdings Mgmt. Corp.,* Docket No. C-4264, para. 4 (F.T.C. Sept. 9, 2009).

8 Complaint, *In the Matter of Myspace LLC,* Docket No. C-4369 (F.T.C. Sept. 11, 2012).

9 Federal Trade Commission, FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising, at 39 (Feb. 2009), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf.

10 See, for example, Solove and Harzog, *supra* note 4.

That said, recent years have brought a flurry of federal action related to cybersecurity. In 2015, Congress enacted the Cybersecurity Information Sharing Act (CISA),[11] which seeks to encourage cyberthreat information sharing within the private sector and between the private and public sectors by providing certain liability shields related to such sharing. CISA also authorises network monitoring and certain other defensive measures, notwithstanding any other provision of law. In addition to CISA, Presidents Obama and Trump have issued a series of executive orders concerning cybersecurity, which have, among other things, directed the Department of Homeland Security and a number of other agencies to take steps to address cybersecurity and protect critical infrastructure and directed the National Institute of Standards and Technology (NIST) to develop a cybersecurity framework.[12] The latter, in particular, has been a noteworthy development: while the NIST Cybersecurity Framework provides voluntary guidance to help organisations manage cybersecurity risks, 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 proprietary business data.

Specific regulatory areas – federal law

Along with the FTC's application of its general authority to privacy-related harms, the United States also has a number of specific federal privacy and data security laws for the types of citizen and consumer data that are most sensitive and at risk. These laws grant various federal agencies rule making, oversight, and enforcement authority, and these agencies often issue policy guidance on both general and specific privacy topics. In particular, Congress has passed robust laws that prescribe specific statutory standards for protecting the following types of information:

a financial information;
b healthcare information;
c information about children;
d telephone, internet and other electronic communications and records; and
e credit and consumer reports.

We briefly examine each of these categories, and the agencies with primary enforcement responsibility for them, below.

Financial information

The Financial Services Modernisation Act of 1999, more commonly known as the Gramm-Leach-Bliley Act (GLBA),[13] addresses financial data privacy and security by establishing standards pursuant to which financial institutions must safeguard and store their customers' 'non-public personal information' (or 'personally identifiable financial information'). In brief, the GLBA requires financial institutions to notify consumers of their policies and practices regarding the disclosure of personal information; to prohibit the

11 Cybersecurity Information Sharing Act of 2015, Pub. L. No. 114 – 113, 129 Stat. 2936 (codified at 6 U.S.C. §§ 1501 – 1510).

12 Exec. Order No. 13636, 78 F.R. 11737 (2013); Exec. Order No. 13718, 81 F.R. 7441 (2016); Exec. Order No. 13800, 82 F.R. 22391 (2017); Exec. Order No. 13873,84 F.R. 22689 (2019).

13 Gramm-Leach-Bliley Act, Pub. L. No. 106 – 102, 113 Stat. 1338 (codified and amended at scattered sections of 12 and 15 U.S.C. (2015)).

disclosure of such data to unaffiliated third parties, unless consumers have the right to opt out or other exceptions apply; and to establish safeguards to protect the security of personal information. The GLBA and its implementing regulations further require certain financial institutions to notify regulators and data subjects after breaches implicating non-public personal information.

Various financial regulators, such as the federal banking regulators (e.g., the Federal Reserve, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency) and the Securities and Exchange Commission (SEC), have authority to enforce consumer privacy under the GLBA for smaller banks, while the FTC (for non-bank financial institutions) and the Consumer Financial Protection Bureau (CFPB) (for larger banks and non-bank financial institutions) do as well.

The SEC has also increasingly used its broad investigative and enforcement powers over public companies who have suffered cybersecurity incidents. In doing so, the SEC has relied on multiple theories, including that material risks were not appropriately disclosed and reported pursuant to the agency's guidance on how and when to do so 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. Of particular note, in 2018, the SEC published interpretive guidance to assist publicly traded companies in disclosing their material cybersecurity risks and incidents to investors.[14] 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.

Healthcare information

For healthcare privacy, entities within the Department of Health and Human Services (HHS) administer and enforce the Health Insurance Portability and Accountability Act of 1996 (HIPAA),[15] as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH).[16] Congress enacted HIPAA to create national standards for electronic healthcare transactions, and HHS has promulgated regulations to protect the privacy and security of personal health information. In general, HIPAA and its implementing regulations state that patients generally have to opt in before covered organisations can share the patients' information with other organisations.

HIPAA's healthcare coverage is quite broad. It defines 'protected health information,' often referred to as PHI, as 'individually identifiable health information [. . .] transmitted or maintained in electronic media' or in 'any other form or medium'.[17] 'Individually

14 SEC Statement and Guidance on Public Cybersecurity Disclosures, 17 C.F.R. §§ 229, 249 (2018).

15 Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified and amended in scattered sections of 18, 26, 29, and 42 U.S.C. (2012)).

16 Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 226, 467 (codified in scattered sections of 42 U.S.C. (2009)).

17 45 C.F.R. § 160.103.

identifiable health information' is in turn defined as 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.[18] Notably, HIPAA does not apply to 'de-identified' data.

With respect to organisations, HIPAA places obligations on '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.[19] Moreover, to safeguard PHI, 'business associates' are required to enter into agreements, called business associate agreements. A business associate is defined as 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).[20] Such agreements require business associates to use and disclose PHI only as permitted or required by the 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. The agreements also include numerous other provisions regarding the confidentiality, integrity and availability of electronic PHI.

HIPAA and HITECH not only restrict access to and use of PHI, but also impose stringent information security standards. In particular, HHS 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.

Information about children

The Children's Online Privacy Protection Act of 1998 (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. The FTC is generally responsible for enforcing COPPA's requirements, which include, among other things, 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.[21]

Telephone, internet, and other electronic communications and records

A number of legal regimes address communications and other electronic privacy and security, and only the briefest discussion of this highly technical area of law is possible here. In short, some of the key statutory schemes are as follows:

18 45 C.F.R. § 160.103.

19 45 C.F.R. § 164.504(f)(3)(iii).

20 45 C.F.R. § 164.103.

21 Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501 - 6505.

a the Electronic Communications Privacy Act of 1986 (ECPA) protects the privacy and security of the content of certain electronic communications and related records;[22]

b the Computer Fraud and Abuse Act (CFAA) 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;[23]

c various sections of the Communications Act protect telecommunications information, including what is known as customer proprietary network information, or CPNI;[24]

d the Telephone Consumer Protection Act (TCPA) governs robocalls;[25] and

e the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act governs commercial email messages, generally permitting companies to send commercial emails to anyone provided that: 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. (Text messages generally require express written consent, and are thus a significant class action risk area.)[26]

The Federal Communications Commission (FCC) is the primary regulator for communications privacy issues, although it shares jurisdiction with the FTC on certain issues, including notably the TCPA.

Credit and consumer reports

The Fair Credit Reporting Act (FCRA),[27] as amended by the Fair and Accurate Credit Transactions Act of 2003,[28] 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 CFPB, FTC and federal banking regulators (e.g., the Federal Reserve, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency) share authority for enforcing FCRA, which mandates accurate and relevant data collection to give

22 Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified in scattered sections of 18 U.S.C. (1986)).

23 Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (1984).

24 Communications Act of 1934, Pub. L. No. 73-416, 48 Stat. 1064 (codified in scattered sections of 47 U.S.C. (1934)).

25 Telephone Consumer Protection Act of 1991, Pub. L. No. 102-243, 105 Stat. 2394 (codified at 47 U.S.C. § 227 (1991)).

26 Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, 15 U.S.C. § § 7701 – 7713 (2003); 18 U.S.C. § 1037 (2003

27 Fair Credit Reporting Act, 12 U.S.C. §§ 1830 – 1831 (1970); 15 U.S.C. § 1681 et seq. (1970).

28 Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, 117 Stat. 1952 (codified as amended at 15 U.S.C. §§ 1681c–1, 1681j, 1681 s–3 (2010)); 20 U.S.C. § 9701 - 9708 (2003)).

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.[29]

ii Privacy and data protection legislation and standards – state law

Oversight of privacy is by no means exclusively the province of the federal government. All 50 US states also engage in some form of privacy and data protection regulation, with particular emphasis on data security and breach notifications. Moreover, state attorneys general have become increasingly active with respect to privacy and data protection matters, often drawing on authorities and mandates similar to those of the FTC. Of particular note, as the largest of the US states, the home to Silicon Valley, and a frequent regulatory innovator, California continues to be a bellwether for US privacy and data protection legislation, with businesses across the United States often applying its regulatory approaches, whether or not they are jurisdictionally required to do so.[30] (To this end, Section III, below, will discuss the new and highly significant California Consumer Privacy Act of 2018.)

Cybersecurity and data breaches – state law

The United States was unquestionably a world leader in establishing information security and data breach notification mandates, and the states played an integral, if not the integral, role. Although the federal government did not – and still has not – put in place a general national standard, all 50 states, the District of Columbia, and other US jurisdictions have imposed their own affirmative data breach notification requirements on private entities that collect or process personal data. California, as is so often the case, was the first: in 2003 the California legislature required companies to notify individuals whose personal information was compromised or improperly acquired. Other states soon followed, and companies who have had nationwide data breaches must now research a number of different laws – which are largely similar, but differ in subtle and important ways – to determine their notification obligations.

In addition to the data breach notification laws, states have also imposed affirmative administrative, technical and physical safeguards to protect the security of sensitive personal information.[31] For example, Massachusetts regulations require regulated entities to have a comprehensive, written information security programme and vendor security controls.[32] Likewise, as discussed below, the California Consumer Privacy Act (discussed below) contains security requirements, and New York has recently enacted a preliminary set of general safeguards, to say nothing of the section-specific cybersecurity rule issued by New York's Department of Financial Services (DFS). In short, absent pre-emptive federal legislation, we should expect to see states continuing to pass new legislation in this area, creating an increasingly complicated patchwork quilt of state laws for companies to navigate.

29 Fair Credit Reporting Act, 15 U.S.C. § 621.

30 State of California Department of Justice, Privacy Laws, oag.ca.gov/privacy/privacy-laws.

31 National Conference of State Legislatures, Security Breach Notification Laws, www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

32 201 Mass. Code Regs. 17.00 (West 2009).

General consumer privacy enforcement – 'Little FTCA' analogues

Similar to the FTC, state attorneys general possess the power to bring enforcement actions based on unfair or deceptive trade practices. The source of this power is typically a 'Little FTC Act', which generally prohibits 'unfair or deceptive acts and practices' and authorises the state attorney general to enforce the law. In particular, the little 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. Moreover, in 39 states and the District of Columbia, these statutes include prohibitions against unfair or unconscionable acts, enforceable by consumers and a state agency.

Thus, if one of the sector-specific federal or state laws does not cover a particular category of data or information practice, businesses may still find themselves subject to regulation. In fact, 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 recent years, attorneys general in states such as California, Connecticut and Maryland have formally created units charged with the oversight of privacy, and New York has created a unit to oversee the internet and technology.

Specific regulatory areas – state laws

While, as described above, the federal government has enacted a number of privacy and data protection laws that target particular industries, activities and information types, the diversity of data laws is even greater at the state level. In the areas of online privacy and data security alone, state legislatures have passed laws covering a broad array of privacy-related issues, such as biometric information, cyberstalking,[33] data disposal,[34] privacy policies, employer access to employee social media accounts,[35] unsolicited commercial communications[36] and electronic solicitation of children,[37] to name just a few. State attorneys general also frequently issue policy guidance on specific privacy topics. For instance, like the FTC, California has also issued best-practice recommendations for mobile apps and platforms.

While a detailed discussion of all of the state laws and regulations is beyond the scope of this chapter, discussion of a couple of exemplary categories should illustrate their importance.

First, consider cybersecurity standards. New York's Department of Financial Services (DFS) is a key regulator here, recently promulgating safeguards that require banks, insurance companies and other financial service institutions it regulates to create and maintain a

33 National Conference of State Legislatures, Cybersecurity Legislation 2016, www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2016.aspx.

34 National Conference of State Legislatures, Data Disposal Laws, www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx.

35 National Conference of State Legislatures, Access to Social Media Usernames and Passwords, www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx.

36 National Conference of State Legislatures, State Laws Relating to Unsolicited Commercial or Bulk E-mail (SPAM), www.ncsl.org/research/telecommunications-and-information-technology/state-spam-laws.aspx.

37 National Conference of State Legislatures, Electronic Solicitation or Luring of Children: State Laws, www.ncsl.org/research/telecommunications-and-information-technology/electronic-solicitation-or-luring-of-children-sta.aspx.

cybersecurity programme designed to protect consumers and New York's financial industry.[38] Thus, as of 28 August 2017, all financial institutions regulated by DFS – which is a wide range of US financial institutions with a presence in many states – must 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. Moreover, as described below, a number of states are promulgating similar or even broader cybersecurity requirements. For instance, New York has built upon the DFS standards by enacting the Stop Hacks and Improve Electronic Data Security Act (SHIELD Act), which, among other things, requires entities that handle private information to implement a data security programme with 'reasonable' administrative, technical and physical safeguards.

Second, consider privacy policies. As is typical, California plays an outsized role here, with its California Online Privacy Protection Act (CalOPPA) almost serving – as many of its laws do – as a de facto national standard and thus affecting businesses operating throughout the United States.[39] In short, CalOPPA requires operators to post a conspicuous privacy policy online that identifies the categories of personally identifiable information that the operator collects about individual consumers. The privacy policy must also detail how the operator responds to a web browser 'do not track' signal. California law also prohibits websites directed to minors from advertising products based on information specific to that minor, and the law further 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.[40]

While California's privacy policy laws are likely the most prominent, they do not stand alone. For instance, Connecticut law requires any person who collects social security numbers in the course of business to create a publicly displayed privacy protection policy that protects the confidentiality of the sensitive number. Nebraska and Pennsylvania have laws that prohibit the use of false and misleading statements in website privacy policies.[41] And there are many other state laws concerning privacy policies, making this an excellent example of the many and diverse regulations that may be relevant to businesses operating across multiple US states.

iii Private litigation

Beyond federal and state regulation and legislation, the highly motivated and aggressive US private plaintiffs' bar adds another element to the complex system of privacy governance in the United States.

Many US laws authorise private plaintiffs to enforce privacy standards, and the possibility of high contingency or attorneys' fees highly incentivise plaintiffs' counsel to develop strategies to use these standards to vindicate commercial privacy rights through

38 N.Y. Comp. Codes R. & Regs. tit. 23, § 500.0 (West 2017).

39 See, for example, National Conference of State Legislatures, Security Breach Notification Laws, www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx, and National Conference of State Legislatures, State Laws Related to Internet Privacy; www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx.

40 Cal. Bus. & Prof. Code §§ 22580 – 22582 (West 2015).

41 National Conference of State Legislatures, State Laws Related to Internet Privacy, www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx.

consumer class action litigation. Indeed, 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 full discussion of the many potential causes of action granted by US law is beyond the scope of this chapter, but a few examples will suffice to show the range of possible lawsuits companies might face. For example, plaintiffs often sue under state 'unfair and deceptive acts and practices' standards, and state law also allows plaintiffs to bring common law tort claims under general misappropriation or negligence theories. Moreover, as mentioned at the outset, US courts have long recognised privacy torts, with the legal scholar William Prosser building on the famed work of Brandeis and Warren to create a taxonomy of four privacy torts in his 1960 article, 'Privacy'[42] – a taxonomy that was later codified in the American Law Institute's famous and influential Restatement (Second) of Torts.[43] Thus, aggrieved parties can today bring a civil suit for invasion of privacy, public disclosure of private facts, 'false light', and appropriation or infringement of the right of publicity or personal likeness. Importantly, these rights protect not only the potential abuse of information, but generally govern its collection and use.

iv Industry self-regulation: company policies and practices

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 the use of consumer data within their sectors, which is then subject to enforcement by both governmental and non-governmental authorities. While there are obviously limits to industry self-regulation, these initiatives have led to such salutary developments as the Digital Advertising Alliance's 'About Advertising' icon and a policy on the opt-out for cookies set forth by the Network Advertising Initiative.[44]

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. It should be noted that 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. To this end, as noted above, California law requires publication or provision of privacy policy in certain instances, and numerous other state and federal laws do as well, including, inter alia, the GLBA (financial data) and HIPAA (health data).[45] In addition, voluntary membership or certification in various self-regulatory initiatives also requires posting of privacy policies, which then become enforceable by the FTC, state attorneys general and private plaintiffs claiming detrimental reliance on those policies.

42 William L. Prosser, Privacy, 48 Calif. L. Rev. 383 (1960).

43 Restatement (Second) of Torts § 652A (Am. Law Inst. 1977).

44 See Digital Advertising Alliance (DAA), Self-Regulatory Program, www.aboutads.info; Network Advertising Initiative, Opt Out Of Interest-Based Advertising, www.networkadvertising.org/choices/?partnerId=1//.

45 National Conference of State Legislatures, State Laws Related to Internet Privacy, http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx.

III THE YEAR IN REVIEW – KEY REGULATORY AND ENFORCEMENT TRENDS

As noted at the outset, the privacy zeitgeist in the United States is shifting. The enactment of the European Union's General Data Protection Regulation, a series of high-profile data breaches, and concerns about misinformation and the misuse of personal information, have created a 'crisis of new technologies' or 'techlash', which has shifted popular views about privacy in the United States and forced the hand of legislators and regulators. The United States is consequently undergoing a period of intense privacy innovation, with the federal government, state governments, and private industry all taking consequential steps to address this new world.

Given the sheer breadth and diversity of activity, this chapter cannot detail every key event in the US privacy and data protection landscape that occurred in the last year. Nonetheless, below we highlight the most important changes, which we believe more than demonstrate how dynamic this area is and will likely continue to be.

i Key federal government privacy and data protection actions

Over the past year, all three branches of the federal government have taken significant steps with respect to privacy and data protection, underscoring the current focus on these issues.

Executive branch – recent enforcement cases

The biggest news with respect to federal privacy regulation over the past year occurred on 24 July 2019, when the FTC announced that Facebook, Inc 'will pay a record-breaking $5 billion penalty, and submit to new restrictions and a modified corporate structure that will hold the company accountable for the decisions it makes about its users' privacy, to settle [FTC] charges that the company violated a 2012 FTC order by deceiving users about their ability to control the privacy of their personal information'.[46] This settlement exemplified the emerging new privacy zeitgeist – as the FTC noted, the US$5 billion penalty was the 'largest ever imposed on any company for violating consumers' privacy', 'almost 20 times greater than the largest privacy or data security penalty ever imposed worldwide', and 'one of the largest penalties ever assessed by the US government for any violation'.[47]

The settlement followed on the heels of a year-long FTC investigation, which led to charges that Facebook 'repeatedly used deceptive disclosures and settings to undermine users' privacy preferences in violation of' a prior FTC consent order, which prohibited Facebook from 'making misrepresentations about the privacy or security of consumers' personal information, and the extent to which it shares personal information'. The FTC's press release further claimed that these allegedly deceptive 'tactics allowed the company to share users' personal information with third-party apps that were downloaded by the user's Facebook "friends"', and that 'Facebook took inadequate steps to deal with apps that it knew were violating its platform policies'.

In addition to the US$5 billion penalty, the FTC entered into a new 20-year settlement order with Facebook. This order was notable for how it required Facebook to put in place a

46 Press Release, FTC, FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook, (Jul. 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions.

47 Id.

new governance structure for managing privacy and data security issues. As the FTC noted, the settlement order 'overhauls the way the company makes privacy decisions by boosting the transparency of decision making and holding Facebook accountable via overlapping channels of compliance'.[48] In particular, governance aspects of the settlement order include 'greater accountability at the board of directors level,' including the establishment of an independent privacy committee of Facebook's board of directors, with an independent nominating committee responsible for appointing the members of the privacy committee and a supermajority of the Facebook board of directors required to fire any of them.[49]

Improved 'accountability at the individual level', including by requiring Facebook to 'designate compliance officers who will be responsible for Facebook's privacy program' and by requiring Facebook's CEO and the designated compliance officers independently 'to submit to the FTC quarterly certifications that the company is in compliance with the privacy program mandated by the order, as well as an annual certification that the company is in overall compliance with the order', with false certification subjecting them to individual civil and criminal penalties.[50] 'Strengthen[ed] external oversight of Facebook', by enhancing the 'independent third-party assessor's ability to evaluate the effectiveness of Facebook's privacy program and identify any gaps'.[51]

Various additional privacy and data security requirements, including, among other things, the need to conduct and document privacy reviews of all new or modified products, services, or practices before they are implemented; additional privacy reporting and documentation requirements; a requirement to exercise greater oversight over third-party apps; a requirement to 'implement procedures designed to ensure that Covered Information entered by the User (such as User-generated content) is deleted from servers under [Facebook]'s control, or is de-identified such that it is no longer associated with the User's account or device, within a reasonable period of time (not to exceed 120 days) from the time that the User has deleted such information, or his or her account' subject to certain exceptions; and a requirement to 'establish, implement, and maintain a comprehensive data security program'.[52]

Moreover, the Facebook settlement was not the only record-setting FTC action of the past year. On 27 February 2019, the FTC announced a US$5.7 million civil penalty against makers of the popular free video creation and sharing app, Musical.ly (also now known as TikTok), for violations of COPPA. To date, this is the largest civil penalty the FTC has issued concerning violations of COPPA.[53] The FTC based the penalty on a complaint that alleged that Musical.ly failed to provide appropriate notice and obtain parental consent before collecting information directly from children, despite the fact that Musical.ly not only operated a site that was 'directed to children' under COPPA but also had 'actual knowledge'

48 Id.

49 Id.

50 Id.

51 Id.

52 Id.

53 Press Release, FTC, Video Social Networking App Musical.ly Agrees to Settle FTC Allegations That it Violated Children's Privacy Law, (Feb. 27, 2019), https://www.ftc.gov/news-events/press-releases/2019/02/video-social-networking-app-musically-agrees-settle-ftc;

Proposed Stipulated Order for Civil Penalties, Permanent Injunction, and Other Relief, *United States of America v. Musical.ly, et al.*, No. 2:19-cv-01439 (U.S. Dist. Ct. C.D. of Cal. 2019).

of underage use, due to company practices such as collecting users' dates of birth and grades via their profiles and complaints received from parents who unsuccessfully sought to have their children's information deleted.

The FTC was also not the only federal regulatory agency that had an active year. The SEC has been exercising increasingly aggressive oversight regarding cybersecurity compliance in recent years and the past year was no exception. Building on the SEC's 2018 issuance of new interpretive guidance to assist publicly traded companies in disclosing their material cybersecurity risks and incidents to investors,[54] the SEC's Office of Compliance Inspections and Examinations (OCIE) issued guidance in 2019 identifying the multiple steps it is taking to heighten its enforcement presence for cybersecurity matters.[55] The OCIE further issued two risk alerts in April and May 2019 to provide details regarding specific privacy and cybersecurity issues that regulated entities should focus on to prepare for examinations.[56]

The SEC was also active on the enforcement front. In April 2018, the SEC announced that Altaba Inc (formerly, Yahoo!) had settled cybersecurity allegations brought by the SEC (for US$35 million) in the Commission's first-ever enforcement action against a company for failing to disclose a breach.[57] (Altaba also settled claims with shareholders for US$80 million.) Not long after, the SEC brought an enforcement action against an investment adviser, Voya Financial Inc, for alleged failure to maintain cybersecurity policies and procedures. And, finally, on 24 July 2019, the SEC joined the FTC in announcing a settlement with Facebook – in the SEC's case with Facebook agreeing to pay US$100 million settle charges for 'making misleading disclosures regarding the risk of misuse' of 'user data'.[58]

The FTC's and SEC's increased enforcement emphasis in this area exemplifies the executive branch's broader focus on privacy and data protection issues. The White House has remained engaged, with the President issuing an executive order on 'America's Cybersecurity Workforce', which aimed to close America's cyber workforce gap.[59] The same month, another executive order declared a 'national emergency' related to certain threats against information

54 The SEC suggested that all public companies adopt cyber disclosure controls and procedures that enable companies to: identify cybersecurity risks and incidents; assess and analyse their impact on a company's business; evaluate the significance associated with such risks and incidents; provide for open communications between technical experts and disclosure advisers; make timely disclosures regarding such risks and incidents; and, adopt internal policies to prevent insider trading while the company is investigating a suspected data breach.

55 SEC, Office of Compliance Inspections and Examinations: 2019 Examination Priorities (2019), https://www.sec.gov/files/OCIE%202019%20Priorities.pdf. The OCIE's 2019 Exam Priorities emphasise proper configuration of network storage devices, information security governance, and policies and procedures related to retail trading information security.

56 SEC, Investment Adviser and Broker-Dealer Compliance Issues Related to Regulation S-P – Privacy Notices and Safeguard Policies (Apr. 16, 2019), https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Regulation%20S-P.pdf; SEC, Safeguarding Customer Records and Information in Network Storage – Use of Third Party Security Features (May 23, 2019), https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Network%20Storage.pdf.

57 Press Release, SEC, Altaba, Formerly Known as Yahoo!, Charged With Failing to Disclose Massive Cybersecurity Breach; Agrees To Pay $35 Million, (Apr. 24, 2018), https://www.sec.gov/news/press-release/2018-71.

58 Press Release, SEC, Facebook to Pay $100 Million for Misleading Investors About the Risks it Faced from Misuse of User Data, (Jul. 24, 2019), https://www.sec.gov/news/press-release/2019-140.

59 Exec. Order No. 13800, 82 F.R. 22391 (2017).

and communications technology and services in the United States. It authorised the Department of Commerce to block transactions that involve such services with a 'foreign adversary'.[60]

In September 2018, the Trump administration, through the US Department of Commerce's National Telecommunications and Information Administration, also initiated a process to modernise US privacy policy by requesting comments on a series of privacy principles. The approach laid out in this request signalled a desire to move away from notice-and-comment based approaches to 'refocus' on achieving desirable privacy 'outcomes', such as ensuring that users are 'reasonably informed' and can 'meaningfully express' their privacy preferences, while providing organisations with the flexibility to continue innovating with cutting-edge business models and technologies.[61]

Finally, numerous other federal agencies remain actively engaged, such that businesses operating in the United States should consider whether they would be affected by policies promulgated by a non-traditional privacy or data security regulator. For example, the Department of Homeland Security (DHS) released a 2018 Cybersecurity Strategy and opened a new cyberrisk centre where industry and government can cooperate to evaluate and combat cyberthreats, as well as defend critical US infrastructure.[62] Additionally, in May 2018, the DHS and DOE released a final joint assessment of US incident response capabilities with respect to electricity disruptions in response to President Trump's executive order 13800 on 'Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure'.[63] In March 2019, the DOE further announced funding of up to US$70 million for an institute for advancing cybersecurity in energy efficient manufacturing.[64]

Legislative branch

Unsurprisingly, the popular focus on cybersecurity matters has prompted Congress to join the party. Multiple congressional committees – from the House and the Senate, chaired by Republicans and Democrats – have held high-profile hearings on the possibility of enacting federal privacy legislation, and both industry and civil society are urging Congress to act. There is also widespread support in the Congress for action, such that federal privacy legislation is probably more likely now than it has been at any time in the past generation. Despite the consensus that something needs to be done, however, the support at the time of writing appears to cleave between those who (mirroring industry) want to enact legislation that pre-empts state law such that US businesses are not subject to a patchwork quilt of

60 Exec. Order No. 13873, 84 F.R. 22689 (2019).

61 Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 48,600 (Sept. 26, 2018).

62 Department of Homeland Security Unveils Strategy to Guide Cybersecurity Efforts, U.S. Dep't of Homeland Security (May 15, 2018), https://www.dhs.gov/news/2018/05/15/department-homeland-security-unveils-strategy-guide-cybersecurity-efforts; U.S. Dep't of Homeland Security, U.S. Department Of Homeland Security Cybersecurity Strategy (2018), https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf.

63 U.S. Dep't of Homeland Security, Section 2(e): Assessment of Electricity Disruption Incident Response Capabilities (May 28, 2019), https://www.dhs.gov/publication/section-2e-assessment-electricity-disruption-incident-response-capabilities.

64 DOE Announces $70 Million for Cybersecurity Institute for Energy Efficient Manufacturing, Dept. of Energy (Mar. 26, 2019), https://www.energy.gov/articles/doe-announces-70-million-cybersecurity-institute-energy-efficient-manufacturing.

privacy regulation and those who want to allow states to provide additional privacy rights above a federal floor. The enactment of federal privacy legislation rests on the resolution of this debate, as well as agreement on the particulars of the regulatory scheme.

Judicial branch, including key developments with discovery and disclosure

Finally, the federal courts have also recently decided a number of important cases relevant to privacy and data security, further demonstrating the relevance of the topic.

Of particular note, although it does not directly address commercial data practices, is the Supreme Court's decision in *Carpenter v. United States*.[65] *Carpenter* held that the Fourth Amendment protects an individual's historical cell-site locational information (CSLI), even when the information is in the hands of the phone company. This case could have dramatic implications, as, prior to *Carpenter*, the common understanding was that the Fourth Amendment did not protect information provided to another. By potentially limiting this 'third-party doctrine', the Court recognised that the information age has placed an extraordinary amount of potentially sensitive information in the hands of others, requiring a rethink of foundational doctrinal principles. Thus, while the *Carpenter* Court went out of its way to say that its decision was narrow, limited to CSLI, and did not call into question traditional applications of the third-party doctrine (e.g., to bank and telephone records), the decision nonetheless provides yet another example of how privacy regulation is starting to adapt in face of the recognition of the consequences wrought by new technologies.

The federal courts have also delivered this same message in cases more directly relevant to companies. For example, in January 2019, a federal court in Georgia allowed consumers, payment card issuers, and investors to proceed with class action claims against Equifax for its 2017 data breach. Importantly, the court ruled that the consumer plaintiffs had suffered sufficiently actual and concrete injuries to demonstrate standing, and that the investors had pleaded enough specific factual allegations beyond the mere existence of the data breach to demonstrate (if the allegations were proven true) that Equifax's cybersecurity was 'grossly deficient' and that Equifax's statements regarding its cybersecurity preparedness were thus at least misleading.[66] (Ultimately, Equifax reached a global settlement whereby it paid US$1.4 billion to resolve the outstanding class action and regulatory claims against it.)[67]

Similarly, on 8 August 2019, the Court of Appeals for the Ninth Circuit also allowed a privacy-related class action litigation to move forward, when it held, among other things, that Facebook's alleged violations of the procedural requirements of the Illinois Biometric Privacy Act (discussed below) constituted a concrete and particularised harm sufficient to demonstrate standing.[68] The court cited *Carpenter* for the proposition that 'advances in technology can increase the potential for unreasonable intrusion into personal privacy' in holding that the Act protected the plaintiff's concrete interests in biometric privacy.[69] The court then held that violations of the Act's procedures – which require, among other things, establishing a retention schedule and guidelines for permanently destroying biometric information –

65 138 S. Ct. 2206 (2018).

66 *In re Equifax Inc. Sec. Litig.*, 357 F. Supp. 3d 1189 (N.D. Ga. 2019).

67 Equifax Reaches $1.4B Data Breach Settlement in Consumer Class Action, Law.Com (July 22, 2019), https://www.law.com/2019/07/22/equifax-reaches-1-4-billion-data-breach-settlement-in-consumer-class-action/.

68 *Patel v. Facebook, Inc.*, No. 18-15982, 2019 WL 3727424 (9th Cir. Aug. 8, 2019).

69 *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

actually harmed or materially risked harming those interests. This case thus demonstrates how plaintiffs may have more success establishing privacy harms sufficient to get into court when their allegations concern sensitive information gained via advanced technologies.

Finally, the recent settlement of another case further demonstrates the new ways in which companies may face privacy and data security-related liability. On 31 July 2019, Cisco announced that it had paid US$8.6 million to settle a long-running False Claims Act suit in which the plaintiffs alleged that Cisco had knowingly sold vulnerable video surveillance systems to federal and state governmental entities in violation of contractual requirements to provide information protection.[70] This settlement, which has been termed the first time a company has faced cybersecurity-related liability under the False Claims Act, was reached despite the fact that Cisco claimed 'there is no evidence that any customer's security was ever breached'.[71]

ii Key state privacy and data protection actions

While, as the above demonstrates, the federal government has been very active on privacy and data security matters over the past year, there is a very good case that the real action may not be in Washington DC, but rather in the 50 US states.

The California Consumer Privacy Act (CCPA)

The biggest recent privacy development in the United States – by far – has been California's enactment of the CCPA, a comprehensive privacy bill that commentators have taken to calling 'California's GDPR'. Given California's size and the fact that it is the home of Silicon Valley, the CCPA is having a wide impact and companies across the United States and around the world are considering what it might mean for them.

The CCPA will enter go into effect on 1 January 2020, and will immediately become the most far-reaching privacy or data protection law in the country. In short, the bill's nickname reflects reality, as CCPA shares many attributes with the EU's General Data Protection Regulation (GDPR). And while a full discussion of the lengthy bill is beyond the scope of this chapter, the bill's highlights include the following:

a The CCPA applies to for-profit entities that are doing business in California; that collect or determine the means of processing personal information; and that meet one of three size thresholds.[72]

b The CCPA mandates broad privacy policy disclosure requirements on companies that collect personal data about California residents.[73]

c The CCPA mandates that businesses provide California residents with the rights to access and delete their personal information, as well as the right to stop the sale of their information to third parties.[74]

70 Mike Lasusa, Cisco Inks $8.6M Deal To End Surveillance-Tech FCA Claims, Law360 (Jul 31, 2019, 10:31 PM), https://www.law360.com/articles/1184196/cisco-inks-8-6m-deal-to-end-surveillance-tech-fca-claims.

71 Mark Chandler, A Changed Environment Requires a Changed Approach, Cisco: Cisco Blogs (Jul. 31, 2019), https://blogs.cisco.com/news/a-changed-environment-requires-a-changed-approach.

72 The California Consumer Privacy Act, A.B. 375, 2017 Gen Assemb., Reg. Sess. (Cal. 2018).

73 Id. § 1798.140 (g).

74 Id. § 1798.105 (a), 120 (a).

d The CCPA prohibits businesses from selling personal information of individuals under the age of 16, absent affirmative authorisation.[75]

e The CCPA mandates that businesses not treat consumers differently based on the customers' exercise of their CCPA rights, although businesses are allowed to offer incentives.[76]

f The CCPA provides a private cause of action for certain data breaches that result from a business's violation of the duty to implement and maintain reasonable security procedures and practices.[77]

g The CCPA authorises the California Attorney General to enforce its provisions with statutory fines of up to US$7,500 per violation.[78]

h The CCPA was passed very quickly, and the California legislature has already amended it, with more amendments anticipated. The California Attorney General is also required to provide regulatory guidance on the meaning of many of the Act's provisions. The specific requirements of the CCPA are thus not set in stone, although, as of this writing, businesses are engaged in substantial efforts to prepare for its entry into force.

Other state laws

California has long been a privacy bellwether, as its legislative actions have often prompted other states to follow suit: for example, California was the first state to enact a data breach notification law, and all 50 states now have one. It is thus unsurprising that the passage of the CCPA has prompted numerous other states to consider comprehensive privacy legislation. And while these legislative initiatives fizzled out in some places, the past year has seen the enactment of a number of new laws in the CCPA's wake.

Nevada became the first state to follow the CCPA trend when, on 29 May 2019, it enacted a law that grants consumers the right to opt out of the sale of personal information. While Nevada's law is not as comprehensive as the CCPA, it will enter into force earlier – on 1 October 2019.[79]

Maine was the second state to follow in California's footsteps, with the Governor signing into law the Act to Protect the Privacy of Online Consumer Information on 6 June 2019.[80] Again, this law is not as comprehensive as the CCPA, but it does obligate internet service providers in Maine to obtain permission from their customers before selling or sharing their data with a third party.

Finally, on 25 July 2019, New York enacted the Stop Hacks and Improve Electronic Data Security Act (the SHIELD Act),[81] which updates New York's breach reporting law by, among other things, requiring entities that handle private information to implement a data security programme with 'reasonable' administrative, technical and physical safeguards. While this law is again narrower than the CCPA, it is notable for detailing what constitutes 'reasonable security', laying out with some specificity examples of 'reasonable' safeguards. The SHIELD Act also makes clear that entities in compliance with data security frameworks

75 Id. § 1798.120 (d).

76 Id. § 1798.125 (a).

77 Id. § 1798.140 (w)(2)(B).

78 Id. § 1798.155 (b).

79 S.B. 220, 80th Leg., Reg. Sess. (Nev. 2019).

80 S.P. 275, 129th Leg., Reg. Sess. (Me. 2019).

81 S.B. 5775, Reg. Sess. 2019-2020 (N.Y. 2019).

under certain federal or state laws (such as GLBA and HIPAA) are in compliance with the SHIELD Act. In this regard, the Act mirrors a 2018 Ohio law, which did not establish minimum cybersecurity standards but which did provide companies with a safe harbour for tort liability in data breach actions when they put in place 'administrative, technical, and physical safeguards for the protection of personal information and that reasonably confor[m] to an industry recognised cybersecurity framework'.

Besides taking the lead on enacting broad, cross-sectoral privacy and data security legislation, states are also taking the lead in putting in place other, more focused regulatory regimes. We have discussed some examples of this, such as the New York Department of Financial Services' Cybersecurity Regulation, above, but there are many others. For instance, South Carolina passed a law putting in place prescriptive data security requirements for insurers that went into effect on 1 January 2019,[82] and other states have followed suit, enacting requirements that generally track the Insurance Data Security Model Law adopted by the National Association of Insurance Commissioners (NAIC).

States are also taking the lead in regulating emerging technologies, such as autonomous vehicles. A prime example of this is facial recognition technologies. Texas, Washington and Illinois have already enacted statutes governing biometric data directly, many other states indirectly regulate biometric data by including it in their statutory definitions of personal information, and several other states, including Connecticut, New Hampshire and Alaska, have considered or proposed legislation seeking to regulate biometric data. These laws – which generally require notice and opt-out, limitations on the commercial use of acquired biometric data, destruction of the data after a certain amount of time, and employment of industry standards of care to protect the data – will likely continue to be an area of focus going forward.

State courts

Just as the federal courts have decided a number of recent important privacy and data security cases, so too have state courts. While a complete canvas of all of these decisions is beyond the scope of this chapter, highlighting a couple of examples serves to demonstrate the general point.

First, the Illinois Biometric Information Privacy Act (BIPA) provides a private right of action for aggrieved individuals, and, much like the Ninth Circuit, the Illinois Supreme Court has held that bare procedural violations of the statute are sufficient to establish standing.[83] A wide range of technology companies, including Facebook, Shutterfly, Snapchat and Google, thus finding themselves defending their implementation of facial recognition technology against BIPA claims in Illinois courts.

Second, on 31 May 2019, a trial court in the District of Columbia held that the District of Columbia's attorney general could challenge Facebook's privacy practices. In doing so, the court rejected Facebook's arguments that the court lacked jurisdiction over the California-based company and that the attorney general had failed to adequately plead his claims that the company ran afoul of the district's Consumer Protection Procedures Act.[84]

82 H.R. 4655, 122nd Reg. Sess. (S.C. 2018).

83 740 Ill. Comp. Stat. § 14/1 – 99 (2008); *Rosenbach v. Six Flags Ent. Corp.,* No. 123186, 2019 IL 123186 (Jan. 25, 2019).

84 *District of Columbia v. Facebook Inc.,* 2018 CA 008715B (D.C. Super. Ct., Civ. Div. (Wash.)).

These cases, in short, demonstrate the risks companies face as courts also respond to the shifting privacy zeitgeist.

iii Companies expand oversight of privacy and data security issues

In light of the legal and regulatory trends at the federal and state level identified above – to say nothing of international trends discussed elsewhere in the book – companies are increasingly recognising the importance of showing that they have in place structures to ensure sufficient management and board oversight of privacy, data protection and disruptive technologies.

This is a trend that has been building over time. In recent years, it has become best practice to appoint a chief privacy officer and an IT security officer, to put in place an incident response plan and vendor controls (which may be required by some state laws and in some sectors by federal law), and to provide regular employee training regarding data security. However, as technology advances and companies increasingly view information as a significant strategic opportunity and risk, companies are increasingly sensing that these structures, policies and procedures are insufficient.

Indeed, while not so long ago companies were comfortable with IT and legal departments running the show with respect to privacy issues, they are now increasingly elevating the level of attention these issues receive and involving senior management and the board in oversight and decision making. The examples of this are legion, and here are just a few:

a Microsoft has created a technology and corporate responsibility team that reports to the president and provides guidance to the board and management on ethical business practices, privacy and cybersecurity.[85]

b Microsoft and other companies have put in place internal boards to help oversee and navigate the challenging moral, ethical, and practical issues raised by artificial intelligence.[86]

c Numerous companies, including Walmart, BNY Mellon and AIG, have put in place technology committees of their board, with responsibility to, among other things, review IT planning, strategy, and investment; monitor and provide guidance on technological trends; and review cybersecurity planning and investment.[87]

In short, companies have recognised the changing zeitgeist, and they are increasingly taking steps to create an effective organisational structure and practices to manage, guide and oversee privacy, data protection and disruptive technologies.

85 We see the big picture, Microsoft Corp. (August 23, 2019), https://www.microsoft.com/en-us/corporate-responsibility/governance.

86 AI news and events, Microsoft Corp. (August 23, 2019), https://www.microsoft.com/en-us/ai?activetab=pivot1%3aprimaryr5; SAP Becomes First European Tech Company to Create Ethics Advisory Panel for Artificial Intelligence, SAP News (Sept. 18, 2018), https://news.sap.com/2018/09/sap-first-european-tech-company-ai-ethics-advisory-panel/.

87 Walmart Inc., Technology and Ecommerce Committee Charter (adopted Jun. 2, 2011), https://s2.q4cdn.com/056532643/files/doc_downloads/Gov_Docs/TeCC-Charter[1].pdf; BNY Mellon, Technology Committee: Charter of the Technology Committee of the Board of Directors, The Bank of New York Mellon Corporation (approved Apr. 9, 2019), https://www.bnymellon.com/us/en/who-we-are/corporate-governance/technology-committee.jsp, American International Group, Inc., Technology Committee Charter (effective May 9, 2018), https://www.aig.com/content/dam/aig/america-canada/us/documents/corp-governance/technology-committee-charter-05.09.18.pdf.

IV INTERNATIONAL DATA TRANSFER AND DATA LOCALISATION

The changing privacy zeitgeist has altered not only the privacy and data protection regime within the United States, but it also threatens to change how the United States approaches certain transfers of information between the United States and other countries.

What has not changed is that there are no significant or generally applicable data transfer restrictions in the United States. That said, the United States has taken steps to provide compliance mechanisms for companies that are subject to data transfer restrictions set forth by other countries. In particular, the EU–US Privacy Shield continues to provide a framework for transatlantic data transfers, and the United States was approved in 2012 as the first formal participant in the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules system. The FTC's Office of International Affairs further works with consumer protection agencies globally to promote cooperation, combat cross-border fraud and develop best practices.[88]

The cross-border issue that has seen more recent activity is law enforcement access to extraterritorial data. Historically, the mutual legal assistance treaty (MLAT) system has governed cross-border transfers of data for law enforcement purposes. In recent years, however, the rise of cloud computing has led to more and more data being stored somewhere other than the jurisdiction in which it was created, placing strain on the system as the antiquated MLAT process was insufficiently nimble to keep up with the increased demand. Other countries therefore became increasingly concerned about their inability to obtain timely evidence, as US technology companies frequently held the relevant information but were barred by US law from turning it over to foreign governments without going through the MLAT process.

These issues came to a head when the Supreme Court heard a case concerning whether a search warrant served in the United States could authorise the extraterritorial transfer of customer communications notwithstanding the laws of Ireland. US companies were thus faced with being placed in the middle of a second conflict of law – not only would they be forbidden from turning over information to foreign governments without a formal MLAT request, but they would also have to turn over information to the US government even absent an MLAT request.

Given the prospect of US industry facing this twin dilemma, as well as the desire of foreign governments to address the concerns caused by the current operation of the MLAT process, Congress enacted the Clarifying Lawful Overseas Use of Data Act (the CLOUD Act).[89] The CLOUD Act was designed to serve two purposes. First, it clarified that a US search warrant could compel companies to disclose certain communications and records stored overseas, thereby mooting the case before the Supreme Court. Second, the CLOUD Act addressed the converse issue – foreign government access to information held in the United States – by authorising the executive branch to enter into international agreements that would allow for certain foreign nations to obtain content directly from US companies without going through the MLAT process.

At the time of writing, the United States has still not entered into any CLOUD Act agreements that would facilitate foreign government access to communication held within the United States. Moreover, the CLOUD Act's clarification of the extraterritorial reach of

88 See FTC, Office of International Affairs, www.ftc.gov/about-ftc/bureaus-offices/office-international-affairs. See also FTC, International Consumer Protection, www.ftc.gov/policy/international/international-consumer-protection.

89 Clarifying Lawful Overseas Use of Data Act, 18 U.S.C. §§ 2523, 2713 (2018).

US law enforcement process has caused consternation, as companies that store data outside the United States have been pressed by non-US customers and counterparts to explain whether the CLOUD Act creates new risk that their data may now be within reach of the US government. The US Department of Justice has thus recently taken steps to explain that, in its view, the CLOUD Act broke no new ground and only clarified, rather than expanded, the reach of US law enforcement; and that, in any event, the requirements in the United States for obtaining a warrant for the content of electronic communications are perhaps the toughest in the world and are highly protective of individual privacy.[90]

Thus, it is safe to say that it is still too soon to tell what the impact of the CLOUD Act will be. That said, the CLOUD Act is clearly yet another example of how US lawmakers and regulators are trying to redesign the regulatory structures governing the data economy.

V CONSIDERATIONS FOR FOREIGN ORGANISATIONS AND OUTLOOK

Foreign organisations can face federal or state regulatory or private action if they satisfy normal jurisdictional requirements under US law, which typically require 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, and if a foreign organisation is a publicly traded company, the SEC has jurisdiction. Moreover, US law enforcement and other enforcement agencies have broad ideas about their jurisdiction.[91]

For all these reasons, US law can have a dramatic impact on foreign organisations. And, as a result, we live in interesting times. As detailed above, the US law concerning privacy and data security is quite dynamic, with both federal and state lawmakers and regulators actively considering potentially dramatic new laws and regulations. Foreign organisations are thus recommended to keep careful tabs on US developments, as the requirements may change at any moment.

90 Press Release, U.S. Dep't of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act (April 2019), https://www.justice.gov/opa/press-release/file/1153446/download.

91 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. Companies should also consider possible international data transfer conflicts when crafting their global privacy and data protection compliance programmes. Consideration should be given to whether US operations require access to non-US data, such that non-US data could be considered within the company's lawful control in the United States and thereby subject to production requests irrespective of foreign blocking statutes. The United States respects comity, but a foreign country's blocking statute does not trump a US legal requirement to produce information.

Appendix 1

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.

TOMMY ANGERMAIR

CLEMENS

Tommy Angermair is a partner in the Danish law firm Clemens and the head of the law firm's employment, data protection and corporate immigration law practice group. Tommy is one of the most experienced Danish experts on data protection law (including GDPR) compliance having provided advice on this topic since 2004. Tommy and the rest of Clemens' very experienced data protection team is currently heavily involved in several GDPR compliance projects for mainly medium-sized and large companies, including several large multinationals. Furthermore, Tommy is specialised in corporate immigration law (WPs, business visas for inbound personnel, advising high net worth individuals etc.), which means that he has a profound understanding of the data protection consideration in relation to running an immigration law practice. Tommy Angermair annually speaks at international legal conferences across the globe. Among other things, he is a frequent speaker at the AILA GMS annual conference in the US and the biennial IBA Global Immigration & Nationality Law conference on topics related to immigration, data protection and mobility. He has

contributed to several primarily international publications within his area of expertise, including the chapter on Denmark in the recent editions of the *Global Business Immigration Handbook* and *The Employment Law Review*.

NATALIA BARRERA SILVA

Márquez, Barrera, Castañeda & Ramírez

Natalia Barrera Silva is a law graduate of Pontificia Universidad Javeriana and holds an LLM degree from Columbia University, which 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 Administración.

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

Uría Menéndez Abogados, SLP

Reyes Bermejo is a lawyer based in both the Madrid and Valencia offices 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 Uría Menéndez*) on aspects of and updates relating to data protection regulatory issues and case law.

FRANCESCA BLYTHE

Sidley Austin LLP

Francesca Blythe is a senior associate in the London office at Sidley Austin LLP, whose main practice areas are data protection, privacy, cybersecurity, e-commerce and information technology.

SØREN BONDE

CLEMENS

Søren is second year assistant attorney in the Danish law firm Clemens and part of one of the leading and most experienced data protection law practice groups in Denmark. Søren has a background as a legal manager in a multinational IT company headquartered in Denmark. With his background as a Master of Business Law (MSc Law) as well as a Master of Law (LLM), Søren is particularly skilled at the analysis of complex legal issues with a view to obtaining the best possible commercial result. Søren has extensive experience with assisting clients in their purchase and development of IT applications and new technologies in an efficient and pragmatic manner, especially in connection with assessment of legal consequences when developing or utilising new products and technologies in relation to protection of personal and corporate data. Moreover, Søren advises all client types on data protection issues, including in particular compliance assessments and general implementation issues and interpretation of the GDPR, preparation of data processor agreements and privacy policies. In addition, Søren regularly gives presentations on personal data challenges and issues.

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.

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 the European Law Students Association's Turkish branch and is admitted to the Istanbul Bar Association.

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, defense 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 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.

ALEKSANDRA CZARNECKA

Kobylańska Lewoszewski Mednis Sp. J.

Aleksandra Czarnecka is a lawyer working for Kobylańska Lewoszewski Mednis Sp. J. law firm. Before joining Kobylańska Lewoszewski Mednis Sp. J. law firm, Aleksandra was an associate in the TMT/IP law/personal data protection team of an international law firm. She specialises in personal data protection and cybersecurity law. Aleksandra took part in GDPR implementation projects in companies from various sectors, including pharmaceutical, medical, e-commerce and technological sectors, as well as project on implementing AML Directive (IV) for entity from banking sector. She also provided advice in the field of transferring data to states outside the European Union.

Aleksandra graduated with honours from the Faculty of Law and Administration at the Warsaw University and the Center for American Law Studies jointly organised by the Georgia State University College of Law, the Emory University School of Law and the Faculty of Law and Administration at the Warsaw University.

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 bachelor's and master's degrees in pharmacy, with a specialisation in pharmaceuticals, and is also a registered patent agent.

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, 2018 and 2019 he was given 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.

MARCELA FLORES GONZÁLEZ

Santamarina y Steta, SC

Ms Flores González obtained her law degree from the Monterrey Institute of Technology and Higher Education in 2016. She is fluent in Spanish and English.

Ms Flores González joined Santamarina y Steta, SC in 2015, and since then her professional practice has been focused on data privacy matters, mergers and acquisitions and other corporate matters.

Ms Flores González practice focuses on data privacy matters, and she advises clients on compliance with data privacy legislation, including the drafting of the required documents to comply with the law; 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, and advising on breaches of personal data confidentiality obligations, among other matters.

CHRISTOPHER C FONZONE

Sidley Austin LLP

Christopher C Fonzone is a partner in Sidley Austin's privacy and cybersecurity group. His practice focuses on a wide range of issues related to information technology and cybersecurity, as well as the management of crisis situations. Before joining Sidley, Chris was deputy assistant and deputy counsel to President Obama and the legal adviser to the National Security Council. Before that, Chris worked at the Departments of Defense and Justice and as a law clerk to Justice Stephen Breyer of the US Supreme Court and Judge J Harvie Wilkinson III of the US Court of Appeals for the Fourth Circuit. Chris has lectured and taught classes at a variety of law schools, and his writing on national security and privacy and cybersecurity topics has been published in many forums, including the *Washington Post*, *The Hill*, *Newsweek*, *Lawfare* and *Just Security*.

ADRIÁN FURMAN

Bomchil

Adrián Furman is a partner in the mergers and acquisitions and entertainment law departments and in charge of 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.

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 was 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*, *Legal 500* and *Best Lawyers*, and by the Latin American Corporate Counsel Association and Client Choice Awards.

KAROLINA GAŁĘZOWSKA

Kobylańska Lewoszewski Mednis Sp. J.

Karolina Gałęzowska is a lawyer working for Kobylańska Lewoszewski Mednis Sp. J. law firm. Before joining Kobylańska Lewoszewski Mednis Sp. J, Karolina was a senior associate in the TMT team of an international law firm. She specialises in administrative (public) law, as well as data protection and telecommunications law.

She provides advice on data protection and e-privacy for the banking, telecoms, petrol and e-commerce sector, credit information agencies and public entities.

She participated in numerous GDPR implementation projects and in the implementation of the GDPR into the domestic legal system, co-authoring amendments and derogations for more than 30 legal acts. Her experience includes proceedings before the Polish DPA and the President of the Office of Electronic Communications. Karolina is the author or co-author of a number of publications on data privacy and is a member of the IoT working group of the Ministry of Digital Affairs.

She is a law graduate of the College of Interdisciplinary Individual Studies in the Humanities and Social Sciences at the University of Warsaw. She is currently a PhD candidate, working on a thesis on international data protection supervision.

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.

FLORIAN GROOTHUIS

Winheller Attorneys At Law & Tax Advisors

Florian Groothuis is scientific researcher at the IP/IT department at Winheller Attorneys at Law & Tax Advisors and is specialised in data protection law and IT related legal matters.

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. In addition, 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 cyber risk 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.

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 and 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 KINIKOĞLU

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 master's 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 Mednis 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 Mednis Sp. J. 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.

MARCIN LEWOSZEWSKI

Kobylańska Lewoszewski Mednis 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 GIODO (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 protection lawyers. He is also on the editorial board of *e-Health Law & Policy* and also assists with dplegal ('data privacy legal'), a networking group of in-house lawyers in life sciences companies examining international data protection issues. 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 and spent a year at the UK's Financial Law Panel (established by the Bank of England), as assistant to the chief executive working on regulatory issues with online financial services.

LETICIA LÓPEZ-LAPUENTE

Uría Menéndez Abogados, SLP

Leticia López-Lapuente joined Uría Menéndez in 2004. She was named partner in 2019. She heads the firm's data protection and e-commerce area and also 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.

MICHAEL MORRIS

Allens

Michael specialises in all corporate, commercial and regulatory aspects of technology, telecommunications, intellectual property and the data life cycle. He has 20 years' experience across a range of ICT sector, IP and data issues in Australia, Europe, Singapore and Papua New Guinea. He is particularly experienced in large projects that involve the procurement or outsourcing of ICT, business process outsourcing, ICT system separations, business transformation, and corporate transactions and projects in the ICT sector and data market.

He also regularly advises clients across all industry sectors and government on cybersecurity issues, data protection, data commercialisation, data governance, dealing with data breaches, IP protection and IP commercialisation.

ALAN CHARLES RAUL

Sidley Austin LLP

Alan Raul is the founder and leader 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. He also advises companies on their digital governance strategies and cyber crisis management. 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 Technology 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).

Hugh Reeves speaks English, French and German. He is registered with the Vaud Bar Registry and admitted to practise in all of Switzerland.

SHERI PORATH ROCKWELL

Sidley Austin LLP

Sheri Porath Rockwell is a lawyer in the firm's Los Angeles office and a member of the privacy and cybersecurity practice and the complex commercial litigation practice. She advises clients on a variety of federal and state privacy issues, and is CIPP-US certified. Sheri earned her JD from the University of Southern California Gould School of Law and her BA, with honours, from the University of California, Berkeley.

CAMILLA SAND FINK

CLEMENS

Camilla is a senior lawyer in the Danish law firm Clemens and part of one of the leading and most experienced data protection law practice groups in Denmark. Camilla has a background as corporate legal counsel and GDPR compliance project manager in an international energy group headquartered in Denmark. Camilla provides data protection advice within all areas of data protection law, including compliance assessments and implementation issues, interpretation of the GDPR as well as handling of rights request, data breaches and complaints to the Danish Data Protection Agency. Camilla advises all client types and has been involved in several national and international compliance projects for mainly medium-sized and large companies and multinationals. In addition, Camilla regularly gives presentations on personal data challenges and issues. Finally, Camilla has extensive litigation experience and right to appear before the Danish High Courts.

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 Vaud Bar Registry and admitted to practise in all of Switzerland.

SNEZHANA STADNIK TAPIA

Sidley Austin LLP

Snezhana Stadnik Tapia is an associate in Sidley Austin's privacy and cybersecurity practice, where she assists clients with privacy and cybersecurity issues. Snezhana received her law degree from New York University School of Law, where she was an online editor for the *Journal of International Law and Politics*. During law school, Snezhana explored transnational legal and regulatory issues with respect to global digital technologies as a research assistant and worked on data governance and privacy issues at an urban innovation tech company.

OLGA STEPANOVA

Winheller Attorneys At Law & Tax Advisors

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.

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).

Monique Sturny speaks German, English and French. She is registered with the Zurich Bar Registry and admitted to practise in all of Switzerland.

ADITI SUBRAMANIAM

Subramaniam & Associates

Aditi Subramaniam has a bachelor's degree in English literature from the University of Delhi, a bachelor's degree in law from the University of Oxford, and a master's degree in law (LLM) from Columbia Law School. She is qualified to practise law in the territories of India and is awaiting her registration to the New York Bar, having recently passed the New York Bar Examination. 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 sector in *IFLR1000* as a 'leading lawyer' and has also been listed by *Who's Who Legal* as a 'leading business lawyer' in life sciences, business crime defence 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'.

OLIVIER VAN FRAEYENHOVEN

Astrea

Olivier Van Fraeyenhoven is a partner of Astrea. He is active in the field of commercial law and specialises in intellectual property, distribution, trade practices and ICT law. He has 20 years experience in assisting domestic and international clients in distribution law (and all competition related aspects), national and international sales agreements, product liability issues, e-commerce, trade practices, intellectual property (with a focus on trademark), privacy and ICT law related advices, negotiations, litigation matters and contract drafting. With the adoption of the GDPR, he has assisted a large number of clients and their distribution network with the implementation of the new rules. He has also conducted a significant number of Data Privacy Impact Assessment. He has particular experience in the provision of legal advice to major clients in the automotive sector. Apart from this, he acts for clients in general commercial disputes and court surveys.

Olivier graduated from the University of Louvain (UCL 1990, *cum laude*) and also obtained a postgraduate degree in economic law from the University of Brussels (1992). In 1992, he became a member of the Brussels Bar and joined the law firm De Caluwé & Dieryck. In 1993 and 1994 he worked with Texaco Belgium as assistant to the general counsel before joining the Antwerp Bar in 1995 as an associate at Dieryck, Van Looveren & Co, later merged into Buyle Dieryck Van Looveren Maingain. Beginning in 2002, he became a partner at Buyle Dieryck Van Looveren Maingain before joining Lawfort as a partner within the IP, IT and distribution Department (2003–2006). In 2006 he co-founded the law firm Astrea.

Olivier is visiting professor at the Louvain School of Management (Facultés Notre Dame de la Paix) where he teaches IP and distribution law. He has published on matters of distribution law, agency agreements and product liability. He is a regular speaker at seminars.

Olivier is a member of the Antwerp Bar. He speaks Dutch, French and English.

SANJA VUKINA

Vukina & Partners Ltd

Attorney at law Sanja Vukina is the founder and managing partner in law firm Vukina & Partners Ltd. Mrs Vukina has been registered with the Croatian State Intellectual Property Office as a patent and trademark attorney since 1993. She is also a member of the Executive Board of the Croatian Association of Patent and Trademark Attorneys, a European patent attorney, Croatian representative with the European Patent Institute and a certified trainer for licensing agreements for the Licensing Executives Society International. In 2017, she received the Client Choice award for Croatia, being recognised by the clients as the best local attorney in the field of intellectual property and trademark law.

Mrs Vukina mainly provides legal services regarding intellectual property-related rights, with a particular focus on the implementation of business solutions through commercial contracts and corporate regulations regarding the creation, application and exercise of IP related rights.

Mrs Vukina also advises on issues relating to applicable data protection legislation, such as data protection compliance and innovative tailor-made solutions regarding the processing of personal data for companies, particularly the processing of special categories of personal data concerning health, such as that processed within the pharmaceutical and healthcare businesses.

Due to her professional experience as a patent and trademark attorney registered with the Croatian State Intellectual Property Office and Croatian Copyright Association, Mrs Vukina has a particular insight regarding copyright protection, trademarks, pharmaceutical product patents and resolution of disputes in relation to intellectual property rights.

HONGQUAN (SAMUEL) YANG

AnJie Law Firm

Hongquan (Samuel) Yang leads AnJie Law Firm's technology, data protection and cybersecurity practice. He has worked as in-house counsel and external lawyer in the technology, media and telecoms sector for more than 16 years and is regarded as a true expert in these areas in China. He advises clients on a wide range of regulatory, commercial and corporate matters, especially in the areas of telecommunications, cybersecurity, data protection, the internet, social networking, online games, hardware and software, technology procurement, transfer and outsourcing, distribution and licensing, and other technology-related matters. He also advises clients on compliance and employment matters.

Samuel mainly serves Fortune 500 companies, large state-owned enterprises and leading Chinese internet companies. Samuel is a regular contributor to many legal journals and his publications regarding Chinese data protection and cybersecurity laws are well-received and widely reproduced.

FRANCISCO ZAPPA

Bomchil

Francisco Zappa is a senior lawyer in the mergers and acquisitions and entertainment law departments. He joined 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

CONTRIBUTORS' 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

ANJIE LAW FIRM

19/F, Tower D1
Liangmaqiao Diplomatic Office Building
No. 19 Dongfangdonglu
Chaoyang District
Beijing 100600
China
Tel: +86 10 8567 5988
Fax: +86 10 8567 5999
yanghongquan@anjielaw.com
www.anjielaw.com

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
ovf@astrealaw.be
www.astrealaw.be

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

BOMCHIL

Corrientes Avenue 420, 3rd floor
Buenos Aires
Argentina
Tel: +54 11 4321 7500
Fax: +54 11 4321 7555
adrian.furman@bomchil.com
francisco.zappa@bomchil.com
catalina.malara@bomchil.com
www.bomchil.com.ar

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

CLEMENS

Skt. Clemens Straede 7
8000 Aarhus C
Denmark
Tel: +45 87 32 12 50
Fax: +45 87 32 12 51
tma@clemenslaw.dk
csf@clemenslaw.dk
sbo@clemenslaw.dk
www.clemenslaw.dk

KOBYLAŃSKA LEWOSZEWSKI MEDNIS SP. J.

ul. Jana i Jędrzeja Śniadeckich 10
00-656 Warsaw
Poland
Tel: +48 22 25 34567
marcin.lewoszewski@klmlaw.pl.
anna.kobylanska@klmlaw.pl.
karolina.galezowska@klmlaw.pl.
aleksandra.czarnecka@klmlaw.pl.
www.klmlaw.pl

MÁRQUEZ, BARRERA, CASTAÑEDA & RAMÍREZ

Cra 11A No. 97A-19 Of 401
Bogotá
Colombia
Tel: +57 1 675 3548
nbarrera@marquezbarrera.com
www.marquezbarrera.com

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

ul. 1-ya Brestskaya 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
ccruz@s-s.mx
dacosta@s-s.mx
mflores@s-s.mx
www.s-s.mx

SIDLEY AUSTIN LLP

39/F Two International Finance Centre
Central
Hong Kong
Tel: +852 2509 7645
Fax: +852 2509 3110

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

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

1999 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

555 West Fifth Street, Suite 4000
Los Angeles
California 90013
United States
Tel: +1 213 896 6000
Fax: +1 213 896 6600
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
cfonzone@sidley.com
sstadnik@sidley.comsnezhana
www.sidley.com

SK CHAMBERS

9B Jalan Setiapuspa
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 Uría
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

VUKINA & PARTNERS LTD

Prilaz Gjure Deželića 30
Zagreb 10 000
Croatia
Tel: +385 1 7888 941
Fax: +385 1 4874 971
svukina@vukina.hr
https://vukina.hr/en/home/

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

WINHELLER ATTORNEYS AT LAW & TAX ADVISORS

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/en

THE LAW REVIEWS

For more information, please contact info@thelawreviews.co.uk

THE ACQUISITION AND LEVERAGED FINANCE REVIEW
Marc Hanrahan
Milbank Tweed Hadley & McCloy LLP

THE ANTI-BRIBERY AND ANTI-CORRUPTION REVIEW
Mark F Mendelsohn
Paul, Weiss, Rifkind, Wharton & Garrison LLP

THE ASSET MANAGEMENT REVIEW
Paul Dickson
Slaughter and May

THE ASSET TRACING AND RECOVERY REVIEW
Robert Hunter
Edmonds Marshall McMahon Ltd

THE AVIATION LAW REVIEW
Sean Gates
Gates Aviation LLP

THE BANKING LITIGATION LAW REVIEW
Christa Band
Linklaters LLP

THE BANKING REGULATION REVIEW
Jan Putnis
Slaughter and May

THE CARTELS AND LENIENCY REVIEW
John Buretta and John Terzaken
Cravath Swaine & Moore LLP and Simpson Thacher & Bartlett LLP

THE CLASS ACTIONS LAW REVIEW
Camilla Sanger
Slaughter and May

THE COMPLEX COMMERCIAL LITIGATION LAW REVIEW
Steven M Bierman
Sidley Austin LLP

THE CONSUMER FINANCE LAW REVIEW
Rick Fischer, Obrea Poindexter and Jeremy Mandell
Morrison & Foerster

THE CORPORATE GOVERNANCE REVIEW
Willem J L Calkoen
NautaDutilh

THE CORPORATE IMMIGRATION REVIEW
Chris Magrath
Magrath LLP

THE CORPORATE TAX PLANNING LAW REVIEW
Jodi J Schwartz and Swift S O Edgar
Wachtell, Lipton, Rosen & Katz

THE DISPUTE RESOLUTION REVIEW
Damian Taylor
Slaughter and May

THE DOMINANCE AND MONOPOLIES REVIEW
Maurits J F M Dolmans and Henry Mostyn
Cleary Gottlieb Steen & Hamilton LLP

THE E-DISCOVERY AND INFORMATION GOVERNANCE LAW REVIEW
Tess Blair
Morgan, Lewis & Bockius LLP

THE EMPLOYMENT LAW REVIEW
Erika C Collins
Proskauer Rose LLP

THE ENERGY REGULATION AND MARKETS REVIEW
David L Schwartz
Latham & Watkins

THE ENVIRONMENT AND CLIMATE CHANGE LAW REVIEW
Theodore L Garrett
Covington & Burling LLP

THE EXECUTIVE REMUNERATION REVIEW
Arthur Kohn and Janet Cooper
Cleary Gottlieb Steen & Hamilton LLP and Tapestry Compliance

THE FINANCIAL TECHNOLOGY LAW REVIEW
Thomas A Frick
Niederer Kraft Frey

THE FOREIGN INVESTMENT REGULATION REVIEW
Calvin S Goldman QC
Goodmans LLP

THE FRANCHISE LAW REVIEW
Mark Abell
Bird & Bird LLP

THE GAMBLING LAW REVIEW
Carl Rohsler
Memery Crystal

THE GLOBAL DAMAGES REVIEW
Errol Soriano
Duff & Phelps

THE GOVERNMENT PROCUREMENT REVIEW
Jonathan Davey and Amy Gatenby
Addleshaw Goddard LLP

THE HEALTHCARE LAW REVIEW
Sarah Ellson
Fieldfisher LLP

THE INITIAL PUBLIC OFFERINGS LAW REVIEW
David J Goldschmidt
Skadden, Arps, Slate, Meagher & Flom LLP

THE INSOLVENCY REVIEW
Donald S Bernstein
Davis Polk & Wardwell LLP

THE INSURANCE AND REINSURANCE LAW REVIEW
Peter Rogan
Ince & Co

THE INSURANCE DISPUTES LAW REVIEW
Joanna Page
Allen & Overy LLP

THE INTELLECTUAL PROPERTY AND ANTITRUST REVIEW
Thomas Vinje
Clifford Chance LLP

THE INTELLECTUAL PROPERTY REVIEW
Dominick A Conde
Fitzpatrick, Cella, Harper & Scinto

THE INTERNATIONAL ARBITRATION REVIEW
James H Carter
Wilmer Cutler Pickering Hale and Dorr

THE INTERNATIONAL CAPITAL MARKETS REVIEW
Jeffrey Golden
P.R.I.M.E. Finance Foundation

THE INTERNATIONAL INVESTIGATIONS REVIEW
Nicolas Bourtin
Sullivan & Cromwell LLP

THE INTERNATIONAL TRADE LAW REVIEW
Folkert Graafsma and Joris Cornelis
Vermulst Verhaeghe Graafsma & Bronckers (VVGB)

THE INVESTMENT TREATY ARBITRATION REVIEW
Barton Legum
Dentons

THE INWARD INVESTMENT AND INTERNATIONAL TAXATION REVIEW
Tim Sanders
Skadden, Arps, Slate, Meagher & Flom LLP

THE ISLAMIC FINANCE AND MARKETS LAW REVIEW
John Dewar and Munib Hussain
Milbank Tweed Hadley & McCloy LLP

THE LABOUR AND EMPLOYMENT DISPUTES REVIEW
Nicholas Robertson
Mayer Brown

THE LENDING AND SECURED FINANCE REVIEW
Azadeh Nassiri
Slaughter and May

THE LIFE SCIENCES LAW REVIEW
Richard Kingham
Covington & Burling LLP

THE MERGER CONTROL REVIEW
Ilene Knable Gotts
Wachtell, Lipton, Rosen & Katz

THE MERGERS AND ACQUISITIONS REVIEW
Mark Zerdin
Slaughter and May

THE MINING LAW REVIEW
Erik Richer La Flèche
Stikeman Elliott LLP

THE OIL AND GAS LAW REVIEW
Christopher B Strong
Vinson & Elkins LLP

THE PATENT LITIGATION LAW REVIEW
Trevor Cook
WilmerHale

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW
Alan Charles Raul
Sidley Austin LLP

THE PRIVATE COMPETITION ENFORCEMENT REVIEW
Ilene Knable Gotts
Wachtell, Lipton, Rosen & Katz

THE PRIVATE EQUITY REVIEW
Stephen L Ritchie
Kirkland & Ellis LLP

THE PRIVATE WEALTH AND PRIVATE CLIENT REVIEW
John Riches
RMW Law LLP

THE PRODUCT REGULATION AND LIABILITY REVIEW
Chilton Davis Varner and Madison Kitchens
King & Spalding LLP

THE PROFESSIONAL NEGLIGENCE LAW REVIEW
Nicholas Bird
Reynolds Porter Chamberlain LLP

THE PROJECT FINANCE LAW REVIEW
David F Asmus
Sidley Austin LLP

THE PROJECTS AND CONSTRUCTION REVIEW
Júlio César Bueno
Pinheiro Neto Advogados

THE PUBLIC COMPETITION ENFORCEMENT REVIEW
Aidan Synnott
Paul, Weiss, Rifkind, Wharton & Garrison LLP

THE PUBLIC-PRIVATE PARTNERSHIP LAW REVIEW
Bruno Werneck and Mário Saadi
Mattos Filho, Veiga Filho, Marrey Jr e Quiroga Advogados

THE REAL ESTATE INVESTMENT STRUCTURE TAXATION REVIEW
Giuseppe Andrea Giannantonio and Tobias Steinmann
Chiomenti / EPRA

THE REAL ESTATE LAW REVIEW
John Nevin
Slaughter and May

THE REAL ESTATE M&A AND PRIVATE EQUITY REVIEW
Adam Emmerich and Robin Panovka
Wachtell, Lipton, Rosen & Katz

THE RENEWABLE ENERGY LAW REVIEW
Karen B Wong
Milbank

THE RESTRUCTURING REVIEW
Christopher Mallon
Skadden, Arps, Slate, Meagher & Flom LLP

THE SECURITIES LITIGATION REVIEW
William Savitt
Wachtell, Lipton, Rosen & Katz

THE SHAREHOLDER RIGHTS AND ACTIVISM REVIEW
Francis J Aquila
Sullivan & Cromwell LLP

THE SHIPPING LAW REVIEW
George Eddings, Andrew Chamberlain and Holly Colaço
HFW

THE SPORTS LAW REVIEW
András Gurovits
Niederer Kraft Frey

THE TAX DISPUTES AND LITIGATION REVIEW
Simon Whitehead
Joseph Hage Aaronson LLP

THE TECHNOLOGY, MEDIA AND TELECOMMUNICATIONS REVIEW
John P Janka
Latham & Watkins

THE THIRD PARTY LITIGATION FUNDING LAW REVIEW
Leslie Perrin
Calunius Capital LLP

THE TRADEMARKS LAW REVIEW
Jonathan Clegg
Cleveland Scott York

THE TRANSFER PRICING LAW REVIEW
Steve Edge and Dominic Robertson
Slaughter and May

THE TRANSPORT FINANCE LAW REVIEW
Harry Theochari
Norton Rose Fulbright

THE VIRTUAL CURRENCY REGULATION REVIEW
Michael S Sackheim and Nathan A Howell
Sidley Austin LLP

www.TheLawReviews.co.uk

an LBR business

ISBN 978-1-83862-062-2