## CONTENTS

<table>
<thead>
<tr>
<th>Country</th>
<th>Page</th>
<th>Authors/Attorneys</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Introduction</strong></td>
<td>7</td>
<td>Aaron P Simpson and Lisa J Sotto</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hunton Andrews Kurth LLP</td>
</tr>
<tr>
<td><strong>EU overview</strong></td>
<td>11</td>
<td>Aaron P Simpson and Claire François</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hunton Andrews Kurth LLP</td>
</tr>
<tr>
<td><strong>The Privacy Shield</strong></td>
<td>14</td>
<td>Aaron P Simpson</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hunton Andrews Kurth LLP</td>
</tr>
<tr>
<td><strong>Argentina</strong></td>
<td>17</td>
<td>Diego Fernández</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Marval, O’Farrell &amp; Mairal</td>
</tr>
<tr>
<td><strong>Australia</strong></td>
<td>23</td>
<td>Alex Hutchens, Jeremy Perier and Meena Muthuraman</td>
</tr>
<tr>
<td></td>
<td></td>
<td>McCullough Robertson</td>
</tr>
<tr>
<td><strong>Austria</strong></td>
<td>30</td>
<td>Rainer Knyrim</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Knyrim Trieb Attorneys at Law</td>
</tr>
<tr>
<td><strong>Belgium</strong></td>
<td>37</td>
<td>Aaron P Simpson, David Dumont and Laura Léonard</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hunton Andrews Kurth LLP</td>
</tr>
<tr>
<td><strong>Brazil</strong></td>
<td>47</td>
<td>Jorge Cesa, Roberta Feiten and Conrado Steinbruck</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Souto Correa Cesa Lummertz &amp; Amaral Advogados</td>
</tr>
<tr>
<td><strong>Chile</strong></td>
<td>53</td>
<td>Claudio Magliona, Nicolás Yuraszeck and Carlos Araya</td>
</tr>
<tr>
<td></td>
<td></td>
<td>García Magliona &amp; Cía Abogados</td>
</tr>
<tr>
<td><strong>China</strong></td>
<td>59</td>
<td>Vincent Zhang and John Bolin</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Jincheng Tongda &amp; Neal</td>
</tr>
<tr>
<td><strong>Colombia</strong></td>
<td>67</td>
<td>Maria Claudia Martínez Beltrán</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DLA Piper Martínez Beltrán Abogados</td>
</tr>
<tr>
<td><strong>France</strong></td>
<td>73</td>
<td>Benjamin May and Farah Bencheliha</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Aramis</td>
</tr>
<tr>
<td><strong>Germany</strong></td>
<td>81</td>
<td>Peter Huppertz</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hoffmann Liebs Fritsch &amp; Partner</td>
</tr>
<tr>
<td><strong>Greece</strong></td>
<td>87</td>
<td>Vasiliki Christou</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Vasiliki Christou</td>
</tr>
<tr>
<td><strong>India</strong></td>
<td>93</td>
<td>Stephen Mathias and Naqeeb Ahmed Kazia</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Kochhar &amp; Co</td>
</tr>
<tr>
<td><strong>Ireland</strong></td>
<td>99</td>
<td>Anne-Marie Bohan</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Matheson</td>
</tr>
<tr>
<td><strong>Italy</strong></td>
<td>108</td>
<td>Rocco Panetta and Federico Sartore</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Panet &amp; Associati</td>
</tr>
<tr>
<td><strong>Japan</strong></td>
<td>117</td>
<td>Akemi Suzuki and Tomohiro Sekiguchi</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Nagashima Ohno &amp; Tsunematsu</td>
</tr>
<tr>
<td><strong>Korea</strong></td>
<td>124</td>
<td>Seung Soo Choi and Seungmin Jasmine Jung</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Jipyong LLC</td>
</tr>
<tr>
<td><strong>Lithuania</strong></td>
<td>130</td>
<td>Laimonas Marcinkevičius</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Juridicon Law Firm</td>
</tr>
<tr>
<td><strong>Malta</strong></td>
<td>137</td>
<td>Ian Gauci and Michele Tufigno</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Gati Tufigno Gauci Advocates</td>
</tr>
<tr>
<td><strong>Mexico</strong></td>
<td>144</td>
<td>Gustavo A Alcocer and Abraham Díaz Arceo</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Olivares</td>
</tr>
<tr>
<td><strong>Portugal</strong></td>
<td>150</td>
<td>Helena Tapp Barroso, João Alfredo Afonso and Tiago Félix da Costa</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Morais Leitão, Galvão Teles, Soares da Silva &amp; Associados</td>
</tr>
<tr>
<td><strong>Russia</strong></td>
<td>157</td>
<td>Ksenia Andreeva, Anastasia Dergacheva, Anastasia Kiselev, Vasilia Strizh and Brian Zimblere</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Morgan, Lewis &amp; Bockius LLP</td>
</tr>
<tr>
<td><strong>Serbia</strong></td>
<td>164</td>
<td>Bogdan Ivanisević and Milica Basta</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BDK Advokati</td>
</tr>
<tr>
<td><strong>Singapore</strong></td>
<td>169</td>
<td>Lim Chong Kin</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Drew &amp; Napier LLC</td>
</tr>
<tr>
<td><strong>Spain</strong></td>
<td>184</td>
<td>Alejandro Padin, Daniel Caccamo, Katiana Otero, Álvaro Blanco, Pilar Vargas, Raquel Gómez and Laura Cantero</td>
</tr>
<tr>
<td></td>
<td></td>
<td>J&amp;A Garrigues</td>
</tr>
<tr>
<td><strong>Sweden</strong></td>
<td>192</td>
<td>Henrik Nilsson</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Wesslau Söderqvist Advokatbyrå</td>
</tr>
<tr>
<td><strong>Switzerland</strong></td>
<td>198</td>
<td>Lukas Morsch and Leo Rusterholz</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lenz &amp; Staehelin</td>
</tr>
<tr>
<td>Region</td>
<td>Page</td>
<td>Authors</td>
</tr>
<tr>
<td>-----------</td>
<td>------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Taiwan</td>
<td>206</td>
<td>Yulan Kuo, Jane Wang, Brian, Hsiang-Yang Hsieh and Ruby, Ming-Chuang Wang</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Formosa Transnational Attorneys at Law</td>
</tr>
<tr>
<td>Turkey</td>
<td>212</td>
<td>Ozan Karaduman and Selin Başaran Savuran</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Gün + Partners</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>219</td>
<td>Aaron P Simpson and James Henderson</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hunton Andrews Kurth LLP</td>
</tr>
<tr>
<td>United States</td>
<td>226</td>
<td>Lisa J Sotto and Aaron P Simpson</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hunton Andrews Kurth LLP</td>
</tr>
</tbody>
</table>
Preface

Data Protection & Privacy 2019
Seventh edition

Getting the Deal Through is delighted to publish the seventh edition of Data Protection & Privacy, which is available in print, as an e-book and online at www.gettingthedealthrough.com.

Getting the Deal Through provides international expert analysis in key areas of law, practice and regulation for corporate counsel, cross-border legal practitioners, and company directors and officers.

Throughout this edition, and following the unique Getting the Deal Through format, the same key questions are answered by leading practitioners in each of the jurisdictions featured. Our coverage this year includes new chapters on Argentina, Colombia, Greece, Korea, Malta and Taiwan.

Getting the Deal Through titles are published annually in print. Please ensure you are referring to the latest edition or to the online version at www.gettingthedealthrough.com.

Every effort has been made to cover all matters of concern to readers. However, specific legal advice should always be sought from experienced local advisers.

Getting the Deal Through gratefully acknowledges the efforts of all the contributors to this volume, who were chosen for their recognised expertise. We also extend special thanks to the contributing editors, Aaron P Simpson and Lisa J Sotto of Hunton Andrews Kurth LLP, for their continued assistance with this volume.

GETTING THE DEAL THROUGH

London
July 2018

www.gettingthedealthrough.com

© Law Business Research 2018
Singapore

Lim Chong Kin
Drew & Napier LLC

Law and the regulatory authority

1 Legislative framework

Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments on privacy or data protection?

Prior to the enactment of the Personal Data Protection Act 2012 (No. 26 of 2012) (PDPA), Singapore did not have an overarching law governing the protection of personally identifiable information. The collection, use, disclosure and care of personal data in Singapore were regulated to a certain extent by a patchwork of laws including common law, sector-specific legislation and various self-regulatory or co-regulatory codes. These existing sector-specific data protection frameworks will continue to operate alongside the PDPA.

The PDPA was implemented in three phases. On 2 January 2013, selected provisions of the PDPA came into operation. These include provisions that:

- set out the scope and interpretation of the PDPA;
- provide for the establishment of the Personal Data Protection Commission (PDPC) and the Data Protection Advisory Committee (DPAC); and
- provide for the establishment of Do-Not-Call (DNC) registers by the PDPC, and other general provisions of the PDPA.

On 2 January 2014, provisions relating to the DNC registry came into force; and the main data protection provisions under parts III to VI of the PDPA came into effect on 2 July 2014. The main data protection provisions set out the obligations of organisations with respect to the collection, use, disclosure, access to, correction and care of personal data.

Regulations and advisory guidelines under the PDPA deal with specific issues in greater detail.

The Personal Data Protection Regulations 2014 (the PDP Regulations) were gazetted on 19 May 2014. The PDP Regulations supplement the PDPA in three key areas as follows:

- the requirements for transfers of personal data out of Singapore;
- the form, manner and procedures for making and responding to requests for access to or correction of personal data; and
- persons who may exercise rights in relation to disclosure of personal data of deceased individuals.

The other regulations issued under the PDPA are:

- Personal Data Protection (Composition of Offences) Regulations 2015;
- Personal Data Protection (Do Not Call Registry) Regulations 2013;
- Personal Data Protection (Enforcement) Regulations 2014; and
- Personal Data Protection (Appeal) Regulations 2015.

In addition, the PDPC has issued a number of advisory guidelines to provide greater clarity on the interpretation of the PDPA, namely:

- Advisory Guidelines on Key Concepts in the Personal Data Protection Act (Key Concepts Guidelines);
- Advisory Guidelines on the Personal Data Protection Act for Selected Topics (Selected Topics Guidelines);
- Advisory Guidelines on the Do Not Call Provisions;
- Advisory Guidelines for the Telecommunication Sector;
- Advisory Guidelines for the Real Estate Agency Sector;
- Advisory Guidelines for the Education Sector;
- Advisory Guidelines for the Healthcare Sector;
- Advisory Guidelines for the Social Service Sector;
- Advisory Guidelines on Requiring Consent for Marketing Purposes (Marketing Consent Guidelines);
- Advisory Guidelines on Enforcement of Data Protection Provisions (Enforcement Guidelines);
- Advisory Guidelines on Application of PDPA to Election Activities; and
- Advisory Guidelines on In-vehicle Recordings by Transport Services for Hire.

The PDPC has further published general guides to supplement the regulations and guidelines above, which include:

- Guide to Notification;
- Guide to Managing Data Breaches;
- Guide to Securing Personal Data in Electronic Medium;
- Guide on the Practice of Passing Magnetic Stripes of Payment Cards Through a Reader;
- Guide to Handling Access Requests (Access Requests Guide);
- Guide on Data Protection Clauses for Agreements Relating to the Processing of Personal Data;
- Guide on Building Websites for SMEs;
- Guide to Disposal of Personal Data on Physical Medium;
- Guide to Preventing Accidental Disclosure when Processing and Sending Personal Data;
- Guide to Data Sharing;
- Guide to Developing a Data Management Programme;
- Guide to Data Protection Impact Assessments (DPIA Guide);
- Guide to Basic Data Anonymisation Techniques; and
- Guide to Printing Processes for Organisations.

The PDPC has also provided comments and suggestions to the following industry-led guidelines on the PDPA that were developed by the Life Insurance Association Singapore (the LIA) and published on 1 April 2015:

- LIA Code of Practice for Life Insurers on the Singapore Personal Data Protection Act; and

In 2017, the PDPC published its inaugural Personal Data Protection Digest, which is a compendium comprising the PDPC’s grounds of decisions released since 2016, summaries of unpublished cases where a finding of no-breach was found and a collection of data protection-related articles contributed by data protection practitioners. The Personal Data Protection Digest is available on the PDPC’s website.

The formulation of the PDPA framework has taken into account international best practices on data protection. As indicated during the second reading of the PDPA in Parliament, the then Minister of Information, Communications and the Arts had referred to the data protection frameworks in key jurisdictions such as Canada, New Zealand, Hong Kong and the European Union, as well as the OECD Guidelines.
on the Protection of Privacy and Transborder Flows of Personal Data and the APEC Privacy Framework, in developing the PDPA framework.

The PDPC is currently undertaking a review of the PDPA, and has held two public consultations in this regard. First, the Public Consultation for Approaches to Managing Personal Data in the Digital Economy (issued 27 July 2017) sought the public’s views on introducing:

- a Proposed Enhanced Framework for the Collection, Use and Disclosure of Personal Data; and
- a Proposed Mandatory Data Breach Notification Requirement.

Second, the Public Consultation for Managing Unsolicited Commercial Messages and the Provision of Guidance to Support Innovation in the Digital Economy (issued 27 April 2018) sought the public’s views on:

- streamlining the DNC provisions in Part IX of the PDPA and the Spam Control Act into a single legislation governing all unsolicited commercial messages;
- introducing an Enhanced Practical Guidance framework under the PDPA, which allows the PDPC to provide guidance to organisations with greater clarity and certainty; and
- streamlining the exceptions to obtaining consent for the collection, use and disclosure of personal data, found in the Second, Third and Fourth Schedules to the PDPA. The consultation closed on 12 June 2018.

On 20 February 2018, Singapore became the sixth APEC economy to participate in the APEC Cross-Border Privacy Rules (CBPR) system, along with the USA, Mexico, Canada, Japan and the Republic of Korea. Singapore also became the second APEC economy to participate in the APEC Privacy Recognition for Processors (PRP) system. Collectively, the CBPR and PRP systems allow a smoother exchange of personal data among certified organisations in participating economies, and ensure that data protection standards are maintained for consumers in the Asia-Pacific region. The PDPC is currently developing the certification scheme for the CBPR and PRP systems and, in March 2018, called for interested companies to act as assessment bodies for its Data Protection Trustmark Certification scheme. Once the certification scheme is implemented, organisations may start applying for certification under the relevant systems.

2 Data protection authority

Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

The PDPA is administered and enforced by the PDPC. The PDPC was originally established as a statutory body under the PDPA on 1 January 2013 and was under the purview of the Ministry of Communications and Information (the MCI). With effect from 1 October 2016, the PDPC has been subsumed as a department/division under the Infocommunications Media Development Authority (IMDA). The leadership team of the PDPC comprises:

- Mr Tan Kiat How, commissioner, the PDPC;
- Mr Leong Keng Thai, executive chairman of the Data Protection Advisory Committee; and
- Mr Yoong Zee Kin, deputy commissioner, the PDPC.

The PDPC may initiate an investigation to determine whether an organisation is compliant with the PDPA, upon receipt of a complaint or of its own motion. As set out in the Enforcement Guidelines, the factors that the PDPC may consider in deciding whether to commence an investigation include:

- whether the organisation may have failed to comply with all or a significant part of its obligations under the PDPA;
- whether the organisation’s conduct indicates a systemic failure by the organisation to comply with the PDPA or to establish and maintain the necessary policies and procedures to ensure its compliance;
- the number of individuals who are, or may be, affected by the organisation’s conduct;
- the impact of the organisation’s conduct on the complainant or any individual who may be affected;
- whether the organisation had previously contravened the PDPA or may have failed to implement the necessary corrective measures to prevent the recurrence of a previous contravention;
- whether the complainant had previously approached the organisation to seek a resolution of the issues in the complainant but failed to reach a resolution;
- where the PDPC has sought to facilitate dispute resolution between the complainant and the organisation, whether the complainant and the organisation agreed to participate in the dispute resolution process and their conduct during the dispute resolution process and the outcome of the dispute resolution process;
- where the PDPC has commenced a review, whether the organisation has complied with its obligations under the Enforcement Regulations in relation to a review, the organisation’s conduct during the review and the outcome of the review;
- public interest considerations; and
- any other factor that, in the PDPC’s view, indicates that an investigation should or should not be commenced.

In the course of its investigation, the PDPC is empowered to:

- by notice in writing, require any organisation to produce any specified document or to provide any specified information;
- by giving at least two working days’ advance notice of intended entry, enter an organisation’s premises without a warrant; and
- obtain a search warrant to enter an organisation’s premises, and search the premises or any person on the premises (the latter, if there are reasonable grounds for believing that he or she has in his or her possession any document, equipment or article relevant to the investigation), and take possession of, or remove, any document and equipment or article relevant to an investigation.

The PDPC is also empowered to review complaints in relation to access and correction requests (see questions 37 and 38 for more information on access and correction requests).

The PDPA also establishes the DPAC, which advises the PDPC on matters relating to the review and administration of the personal data protection framework, such as key policy and enforcement issues. Currently, the Advisory Committee is headed by Mr Leong Keng Thai, who is also the Deputy Chief Executive Officer of the IMDA. Under him are 13 other members, namely:

- Professor Simon Chesterman, Dean, Faculty of Law, National University of Singapore;
- Mr Hui Choon Kuen, Deputy Chief Counsel Advisory (Civil Division), Attorney General’s Chamber and Dean, AGC Academy;
- Ms Tina Hung, Deputy Chief Executive Officer, National Council of Social Service;
- Mr Mohamed Nasser Ismail, Senior Vice President, Head of Equity Capital Market (SMES) and Head of Capital Market Development, Singapore Stock Exchange;
- Mr Lam Chee Kin, Managing Director & Head, Group Legal Compliance & Secretariat, DBS Bank Ltd;
- Mr Lim Biow Chuan, President, Consumers Association of Singapore;
- Mr Lim Chin Hu, Managing Partner, Stream Global;
- Associate Professor Low Cheng Ooi, Chief Medical Informatics Officer, Ministry of Health and MOH Holdings;
- Professor Steven Miller; Vice Provost (Research), Singapore Management University;
- Ms Ong Seok Leng, Senior Director (Governance Group), Government Technology Agency;
- Mr Teo Chin Hock, Deputy Chief Executive, Cyber Security Agency;
- Mr Lu Cheng Yang, Secretary General Designate, Singapore Chinese Chamber of Commerce and Industry; and
- Mr Kurt Wee, President, Association of Small and Medium Enterprises (ASME).

The addition of members from the banking, healthcare, IT, public and social services sectors and academia is intended to contribute perspectives from each sector to the Advisory Committee.
3 Legal obligations of data protection authority

Are there legal obligations on the data protection authority to cooperate with data protection authorities, or is there a mechanism to resolve different approaches?

The PDPC may enter into a cooperation agreement with a foreign data protection authority for data protection matters such as cross-border cooperation. Cooperation may take the form of information exchange or any other assistance as necessary to assist in the enforcement or administration of data protection laws.

Specifically, section 10 of the PDPA provides that the cooperation agreement has to be entered into for the purposes of:

- facilitating cooperation between the PDPC and another foreign data protection authority in the performance of their respective functions insofar as those functions relate to data protection; and
- avoiding duplication of activities by the PDPC and another foreign data protection authority, being activities involving the enforcement of data protection laws.

In this regard, the cooperation agreement may include provisions to:

- enable the PDPC and the other foreign data protection authority to furnish to each other information in their respective possession if the information is required by the other for the purpose of performance by it of any of its functions;
- provide such other assistance to each other as will facilitate the performance by the other of any of its functions; and
- enable the PDPC and the other foreign data protection authority to forbear to perform any of their respective functions in relation to a matter in circumstances where it is satisfied that the other is performing functions in relation to that matter.

Under the PDPA, the PDPC may only furnish information to a foreign data protection body pursuant to a cooperation agreement if it requires of and obtains from that body an undertaking in writing that the information provided is treated as confidential under the PDPA, the PDPC may only disclose the information to the foreign data protection body if the following conditions are specified:

- the information or documents requested by the foreign data protection body are in the possession of the PDPC;
- the foreign data protection body undertakes to keep the information confidential at all times; and
- the disclosure of the information is not likely to be contrary to the public interest (section 59(3) of the PDPA).

The PDPC is also a participant to the Asia Pacific Economic Corporation Cross-border Privacy Enforcement Arrangement (APEC CPEA), which creates a framework for the voluntary sharing of information and provision of assistance for privacy enforcement-related activities.

4 Breaches of data protection

Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Generally, the powers of the PDPC in the enforcement of any breach of data protection law include:

- powers relating to alternative dispute resolution;
- powers relating to review applications; and
- powers of investigation.

Any individual affected by an organisation’s non-compliance with any of the main data protection provisions may lodge a complaint with the PDPC. Upon receipt of a complaint, the PDPC may investigate or review the matter, or direct the parties as to the appropriate mode of dispute resolution. As mentioned in question 2, the PDPC may commence an investigation in respect of potential breaches of the PDPA further to a complaint, or on its own motion.

In this regard, the Enforcement Guidelines and the public guidance published on the PDPC’s website as of June 2018 states that, when a complaint is received by the PDPC, the PDPC may assess if it can help to address the individual’s concerns by facilitating communications between the individual and the organisation.

If the individual and the organisation are unable to resolve the matter directly and require additional assistance, the PDPC may refer the matter to mediation by a qualified mediator where both the complainant and the organisation involved have consented to the same.

That said, where the PDPC is satisfied that an organisation has breached the main data protection provisions under the PDPA, it is empowered with a wide discretion to issue such remedial directions as it thinks fit. These include directions requiring the organisation to:

- stop collecting, using or disclosing personal data in contravention of the PDPA;
- destroy personal data collected in contravention of the PDPA;
- provide access to or correct personal data, or reduce or make a refund of any fee charged for any access or correction request; or
- pay a financial penalty of up to S$1 million.

In calculating a financial penalty, the PDPC may consider any applicable aggravating or mitigating factors. According to the Enforcement Guidelines and the public guidance published on the PDPC’s website as of June 2018, some of the factors that the PDPC may consider to be aggravating factors include:

- the organisation failing to actively resolve the matter with the individual in an effective and prompt manner;
- intentional, repeated or ongoing breaches of the data protection provisions by an organisation;
- obstructing the PDPC during the course of investigations (such as making efforts to withhold or conceal information requested by the PDPC);
- failing to comply with a previous warning or direction from the PDPC; and
- the organisation is in the business of handling large volumes of sensitive personal data (such as medical or financial data), but failed to put in place adequate safeguards proportional to the harm that might be caused by disclosure of that personal data.

Some of the factors that the PDPC may consider to be mitigating factors include:

- the organisation’s active and prompt resolution of the matter with the individual;
- the organisation taking reasonable steps to prevent or reduce the harm of a breach (such as putting in place strong passwords or encrypting the personal data to prevent unauthorised access);
- the individual affected by the breach has already received a remedy in some other form (for example, through a civil action against the organisation);
- the organisation engaging with the individual in a meaningful manner and having voluntarily offered a remedy to the individual, and that individual having accepted the remedy;
- the organisation taking immediate steps to notify affected individuals of the breach and reduce the damage caused by a breach (such as informing individuals of steps they can take to mitigate risk); and
- the organisation voluntarily notifying the personal data breach to the PDPC as soon as it learned of the breach, and cooperating with the PDPC in its investigations.

On 21 April 2016, the PDPC announced that it had taken its first batch of enforcement actions against 11 organisations for breaching their data protection obligations under the PDPA. Five organisations were issued directions (four of which included financial penalties), while six others were issued warnings. Notably, 10 out of 11 organisations were found to have failed to implement reasonable security arrangements to protect personal data under their possession or control. Since then, the PDPC has also published further enforcement actions taken against organisations that have breached their data protection obligations.

Any person who suffers loss or damage directly as a result of a contravention of any of the main data protection provisions may also commence a private civil action in respect of such loss or damage suffered (see question 38 for further information on such right of private action).

Non-compliance with certain provisions under the PDPA may also constitute an offence, for which a fine or a term of imprisonment may
be imposed. The quantum of the fine and the length of imprisonment (if any) vary, depending on which provisions are breached. For instance, a person found guilty of making requests to obtain access to or correct the personal data of another without authority may be liable on conviction to a fine not exceeding S$5,000 or to imprisonment for a term not exceeding 12 months, or both. Intentionally disposing of, altering, falsifying, concealing or destroying a record containing personal data or information about the collection, use or disclosure of personal data is an offence that may be punishable upon conviction with, in the case of an individual, a fine of up to S$5,000, and in the case of an organisation, a fine of up to S$50,000. The obstruction of PDPC officers (eg, in the course of their investigations) or provision of false statements to the PDPC may be punishable upon conviction with, in the case of an individual, a fine of up to S$10,000 or imprisonment for a term not exceeding 12 months; and in the case of an organisation, a fine of up to S$100,000. See question 27 for more circumstances under which criminal sanctions may be imposed under the PDPA.

Scope

5 Exempt sectors and institutions

Does the data protection law cover all sectors and types of organisation, or are some areas of activity outside its scope?

The PDPA applies to all organisations in Singapore, regardless of their scale or size.

An ‘organisation’ is defined broadly under the PDPA as including any individual, company, association or body of persons, corporate or unincorporated, and whether or not formed or recognised under the law of Singapore, or resident or having an office or place of business in Singapore.

Certain categories of organisations are carved out of the application of the PDPA, such as:

• individuals acting in a personal or domestic capacity;
• employees acting in the course of their employment with an organisation; and
• public agencies, or organisations acting on behalf of a public agency in relation to the collection, use or disclosure of personal data.

The PDPA is intended to set a baseline standard for personal data protection across the private sector, and will operate alongside (and not override) existing laws and regulations. The PDPA provides that the new general data protection framework does not affect any right or obligation under the law, and that in the event of any inconsistency, the provisions of other written laws will prevail. For example, the banking secrecy laws under the Banking Act (Cap. 19) still govern customer information obtained by a bank, and the Telecom Competition Code still governs end-user service information obtained by a telecoms licensee. The PDPC has also published a number of sector-specific advisory guidelines to provide greater clarity on the interpretation of the PDPA in various sectors (see question 3).

6 Communications, marketing and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

Interception of communications and monitoring and surveillance of individuals

To the extent that personal data is collected in the interception of communications and the monitoring and surveillance of individuals, the PDPA applies to the organisation collecting such data. As such, the individual’s consent has to be sought before any such collection takes place, unless such consent is not required (see question 11 for more information on the consent requirement and its exceptions).

For example, the Selected Topics Guidelines indicate that an employer may not need to seek consent for any personal data collected from its monitoring of its employees’ use of company computer network resources as long as such collection is reasonable for the purpose of managing or terminating the employment relationship, although under section 20(4) of the PDPA, it is still required to notify its employees of this purpose for such collection of their personal data.

In relation to CCTV surveillance, the Selected Topics Guidelines explicitly clarify that organisations that install CCTVVs in their premises are required to put up notices informing individuals that CCTVVs are operating in the premises, stating the use and purpose of such surveillance, and if both audio and video recordings are taking place, to state as such, to fulfill their obligation to obtain consent for the collection, use or disclosure of personal data from CCTV footage. This is unless such consent is not required, for example, if the CCTV surveillance is necessary for any investigation or proceedings, insofar as it is reasonable to expect that seeking the consent of the individual would compromise the availability or the accuracy of the personal data. Moreover, the PDPC recommends that while such notices should be placed at points of entry or prominent locations in a venue or a vehicle to enable individuals to have sufficient awareness that CCTV has been deployed in the general locale, they do not have to reveal the exact location of the CCTV cameras. The PDPC also clarifies that an individual may request access to CCTV footage containing his or her image in accordance with the PDPA, unless an exception to this right applies (see question 37 for more details on an individual’s right to access his or her personal data and its limitations). However, the PDPC has also indicated that organisations are generally required to provide access to CCTV footage where the images of other individuals present in the CCTV footage are masked as required (assuming that consent from the other individuals for the disclosure of their personal data has not been obtained).

In addition, where the organisations collecting such personal data via the interception of communications or the performance of surveillance or monitoring activities are public agencies (eg, the Singapore Police Force or the IMDA), they are excluded from the application of the PDPA under section 4(1)(c) of the PDPA. Thus, to the extent that the above exceptions apply, the organisation collecting personal data via interception of communication or monitoring and surveillance of individuals will not have to seek the individuals’ consent prior to such collection.

Apart from the PDPA, there are other regulations that allow for the interception of communications and the monitoring and surveillance of individuals. Below is a non-exhaustive list of such regulations:

- Organisations providing telecommunications services and holding services-based operations licences may have to comply with interception requests by the IMDA and other authorities. Specifically, condition 16 of the IMDA’s standard Services-Based Operator (Individual) (SBO (I)) licence conditions expressly permit disclosure of subscriber information ‘where the disclosure of subscriber information is deemed necessary by the [IMDA] or such other relevant law enforcement or security agencies in order to carry out their respective functions or duties’. Condition 26.1 of the IMDA’s standard SBO (I) licence conditions also require licensees to ‘provide the [IMDA] with any document and information within its knowledge, custody or control, which the [IMDA] may, by notice or direction, require’.
- Section 20 of the Criminal Procedure Code (Cap. 68) empowers the police to require the production of a ‘document or other thing’ (which is necessary for the police investigation) by issuing a written order to ‘the person in whose possession or power the document or thing is believed to be’.
- Section 10 of the Kidnapping Act (Cap. 151) states that the Public Prosecutor may authorise any police officer to, inter alia, ‘intercept any message transmitted or received by telecommunication’ or ‘intercept or listen to any conversation by telephone’.
- Section 15A of the Computer Misuse and Cybersecurity Act (Cap. 50A) states that the Minister may authorise or direct any person or organisation to, inter alia, ‘provide[e] to the Minister or a public officer authorised by him any information (including real-time information) obtained from any computer’. However, upon the coming into force of the Cybersecurity Act 2018 (No. 9 of 2018) on a date yet to be announced, section 15A of the Computer Misuse and Cybersecurity Act will be repealed and replaced with section 23 of the Cybersecurity Act, which provides for the same. The Computer Misuse and Cybersecurity Act will also be renamed the Computer Misuse Act.

Electronic marketing

Section 11 of the Spam Control Act requires any person who ‘sends, causes to be sent or authorises the sending of unsolicited commercial
electronic messages (which include both emails and SMS/MMS) in bulk to comply with certain obligations. These include, among other requirements, that unsolicited commercial electronic messages must contain an unsubscribe facility; by omitting the label '<ADV>' to indicate that the message is an advertisement; and the message must not contain header information that is false or misleading. Section 9 of the Spam Control Act also prohibits electronic messages from being sent to electronic addresses generated or obtained through the use of a dictionary attack or address-harvesting software. The Spam Control Act provides for civil liability (including the grant of an injunction or the award of damages) against parties in breach of these requirements. Statutory damages of up to S$25 per message may be awarded, up to an aggregate of S$1 million (unless the plaintiff proves that his or her actual loss is higher).

In addition to the requirements under the Spam Control Act regarding the sending of spam messages, the PDPA would also apply to personal data collected, used or disclosed through the use of such electronic marketing. Generally, the PDPA requires organisations to obtain consent for a stated purpose to collect, use or disclose the contact information of individuals, unless any exception applies.

With that said, the PDPC is proposing to review, streamline and merge the DNC provisions of the PDPA and the Spam Control Act into a single legislation governing all unsolicited commercial messages, and is currently seeking comments on this as part of its Public Consultation for Managing Unsolicited Commercial Messages and the Provision of Guidance to Support Innovation in the Digital Economy (see question 1).

7 Other laws
Identify any further laws or regulations that provide specific data protection rules for related areas.

Various other legislation in Singapore sets out specific data protection rules, some of which are sector-specific. For instance:

- the Banking Act proscribes the disclosure of customer information by a bank or its officers;
- the Computer Misuse and Cybersecurity Act (which will be renamed the Computer Misuse Act upon the coming into force of the Cybersecurity Act) deals with computer system hackers and other similar forms of unauthorised access or modification to computer systems;
- the Cybersecurity Act establishes a legal framework for the oversight and maintenance of national cybersecurity in Singapore to ensure that computers, systems and data are better protected;
- the Electronic Transactions Act (Cap. 88) provides for the security and use of electronic transactions by criminalising any disclosure of electronic data obtained pursuant to the Act, unless the disclosure is expressly allowed under the Act, required by any written law, or mandated by an order of court;
- the Income Tax Act (Cap. 134) contains provisions that prohibit any person who owns or has control over any documents, information, returns, assessment lists or copies of such lists, to disclose or allow others to have access to such information;
- the Payroll Tax Act (Cap. 213) contains provisions that prohibit any disclosure of information relating to remuneration, payroll tax and income tax;
- the Private Hospitals and Medical Clinics Act (Cap. 248) contains provisions relating to the confidentiality of information held by private hospitals, medical clinics, clinical laboratories and healthcare establishments licensed under the Act;
- the Official Secrets Act (Cap. 213) contains provisions relating to the prevention of disclosure of official documents and information;
- the Statutory Bodies and Government Companies (Protection of Secrecy) Act (Cap. 319) details provisions protecting the secrecy of information of statutory bodies and government companies; and
- the Telecom Competition Code issued under the Telecommunications Act (Cap. 323) contains certain provisions pertaining to the safeguarding of end-user service information. Notably, the IMDA has introduced amendments to the provisions governing end-user service information in the Telecom Competition Code effective 1 July 2014, taking into account that the PDPA will be the primary legislation governing personal data.

On 2 June 2014, the Monetary Authority of Singapore (MAS) also issued its Consultation Paper on the Obligations of Financial Institutions under the Personal Data Protection Act 2012 – Amendments to Notices on Prevention of Money Laundering and Countering the Financing of Terrorism (AML/CFT), which set out its proposed amendments to the MAS Notices on Prevention of Money Laundering and Countering the Financing of Terrorism. The proposed amendments sought to clarify the obligations of financial institutions (FIs) under the AML/CFT requirements in relation to the PDPA. Accordingly, these proposed amendments were incorporated into notices issued by the MAS, pertaining to different classes of FIs, which took effect on 1 July 2014. These amendments apply to the following classes of FIs:

- holders of stored value facilities;
- trust companies;
- approved trustees;
- capital markets intermediaries;
- financial advisers;
- life insurers;
- holders of money-changer’s licence and remittance licence;
- finance companies;
- merchant banks; and
- commercial banks.

Broadly, they make clear that FIs may continue the existing practice of collecting, using and disclosing personal data without customer consent for the purposes of meeting the AML/CFT requirements, and acknowledge customers’ rights under the PDPA to access and correct personal data that is in the possession or under the control of the FI.

8 PII formats
What forms of PII are covered by the law?

All formats of ‘personal data’ are covered under the PDPA, whether electronic or non-electronic, and regardless of the degree of sensitivity. ‘Personal data’ is broadly defined under the PDPA as data, whether true or not, about an individual who can be identified from that data, or from that data and other information to which the organisation has or is likely to have access.

9 Extraterritoriality
Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

Data protection provisions

The data protection provisions under the PDPA generally apply to all organisations that use or disclose personal data in Singapore, regardless of whether they are formed or recognised under Singapore law or whether they are resident or have an office or place of business in Singapore. As such, organisations that are located overseas are still subject to the data protection provisions so long as they collect, use or disclose personal data in Singapore. In addition, organisations that collect personal data overseas and host or process it in Singapore will generally also be subject to the relevant obligations under the PDPA from the point at which such data is brought into Singapore.

Do-not-call provisions

Similarly, the DNC provisions under the PDPA apply to all individuals and organisations sending marketing messages to Singapore telephone numbers, as long as either the sender (when the marketing message is sent) or the recipient (when the marketing message is accessed) is present in Singapore. As an example of its application, the requirement to check the DNC registers would not apply to overseas telecoms service operators sending marketing messages to Singapore subscribers roaming on overseas telecoms networks, because these messages would not be sent or accessed in Singapore. However, organisations in Singapore that outsource their telemarketing activities to overseas organisations and authorise the sending of marketing messages should note that they are still responsible for complying with the DNC provisions, as section 36(1) of the PDPA defines a sender to include a person who causes the message or a voice call containing the message to be sent, or authorises the sending of the message or the making of a voice call containing the message.
For completeness, as mentioned above, the PDPC is proposing to review, streamline and merge the DNC provisions of the PDPA and the Spam Control Act into a single legislation governing all unsolicited commercial messages, and is currently seeking comments on this as part of its Public Consultation for Managing Unsolicited Commercial Messages and the Provision of Guidance to Support Innovation in the Digital Economy (see question 1).

10 Covered uses of PII

Is all processing or use of PII covered? Is a distinction made between those who control or own PII and those who provide PII processing services to owners? Do owners', controllers' and processors' duties differ?

Yes, the PDPA regulates the collection, use and disclosure of personal data by an organisation. An organisation that collects, uses or discloses personal data is accordingly required to comply with the data protection provisions under the PDPA.

A 'data intermediary', however, is exempt from the majority of the data protection provisions under the PDPA. A data intermediary refers to an organisation that processes personal data on behalf of and for the purposes of another organisation (the principal organisation) pursuant to a written contract. A data intermediary is only required to comply with the rules relating to the protection and retention of personal data (see question 12 for further details), while the principal organisation is subject to the full suite of data protection provisions under the PDPA as if it were processing the personal data itself.

A data intermediary that processes personal data in a manner that goes beyond the processing required under the written contract would not be considered a data intermediary, and is subject to the full suite of data protection provisions under the PDPA in respect of that processing.

Legitimate processing of PII

11 Legitimate processing – grounds

Does the law require that the holding of PII be legitimised on specific grounds, for example, to meet the owner's legal obligations or if the individual has provided consent?

Yes, the processing of personal data is expressed in terms of 'collection, use and disclosure' of the same under the PDPA. An individual's consent is required before an organisation can collect, use or disclose such individual's personal data, unless otherwise required or authorised by law. Such consent must be validly obtained and may be either expressly given or deemed to have been given.

For consent to be considered validly given, the organisation must first inform the individual of the purposes for which his or her personal data will be collected, used or disclosed. These purposes have to be what a reasonable person would consider appropriate in the circumstances. Fresh consent would need to be obtained where personal data collected is to be used for a different purpose to which the individual originally consented.

In addition, organisations should note that consent obtained via the following ways does not constitute valid consent for the purpose of the PDPA:

- where consent is obtained as a condition of providing a product or service, and such consent is beyond what is reasonable to provide the product or service to the individual; and
- where false or misleading information is provided, or deceptive or misleading practices are used, in order to obtain or attempt to obtain the individual's consent for collecting, using or disclosing personal data.

The PDPA stipulates that consent is deemed to have been given where the following conditions are satisfied:

- where an individual voluntarily provides his or her personal data to the organisation for a particular purpose; and
- it is reasonable that the individual would voluntarily provide his or her personal data.

Where an individual has given (or is deemed to have given) consent for the disclosure of his or her personal data by Organisation A to Organisation B for a particular purpose, such individual would also be deemed to have given consent to Organisation B for the collection, use or disclosure of his or her personal data for that particular purpose.

While consent is generally needed, the Second, Third and Fourth Schedules to the PDPA provide for specific situations where personal data can be collected, used or disclosed without the individual's consent.

The Second Schedule to the PDPA allows personal data to be collected without consent, for example, where:

- the collection of personal data is necessary for any purpose that is clearly in the interest of the individual, if consent for its collection cannot be obtained in a timely way or the individual would not reasonably be expected to withhold consent;
- the personal data is publicly available;
- the collection of personal data is necessary for any investigation or proceedings, and if it is reasonable to expect that seeking the consent of the individual would compromise the availability or the accuracy of the personal data;
- the collection of personal data is for the purpose of recovery of a debt owed to the organisation by the individual or for the organisation to pay to the individual a debt owed by the organisation;
- the collection of personal data is necessary for the provision of legal services by the organisation to another person, or for the organisation to obtain legal services;
- the personal data is included in a document produced in the course of, and for the purposes of, the individual’s employment, business or profession and collected for the purposes consistent with the purposes for which the document was produced; or
- the personal data is collected by an individual’s employer and the collection is reasonable for the purpose of managing or terminating an employment relationship between the organisation and the individual.

The Third Schedule to the PDPA allows personal data to be used without consent, for example, where:

- the use is necessary for any purpose that is clearly in the interests of the individual and:
  - if consent for its use cannot be obtained in a timely way; or
  - the individual would not reasonably be expected to withhold consent;
- the personal data is publicly available;
- the use is necessary for any investigation or proceedings;
- the personal data is used for an organisation to recover a debt owed to the organisation by the individual or for the organisation to pay to the individual a debt owed by the organisation; or
- the use is necessary for the provision of legal services by the organisation to another person, or for the organisation to obtain legal services.

The Fourth Schedule to the PDPA allows personal data to be disclosed without consent, for example, where:

- the disclosure is necessary for any purpose that is clearly in the interests of the individual if consent for its disclosure cannot be obtained in a timely way;
- the personal data is publicly available;
- the disclosure is necessary for any investigation or proceedings;
- the disclosure is necessary for an organisation to recover a debt owed to the organisation by the individual or for the organisation to pay to the individual a debt owed by the organisation;
- the disclosure is necessary for the provision of legal services by the organisation to another person, or for the organisation to obtain legal services; or
- the personal data is disclosed to any officer of a prescribed law enforcement agency, upon production of written authorisation signed by the head or director of that law enforcement agency or a person of a similar rank, certifying that the personal data is necessary for the purposes of the functions or duties of the officer.

In its Public Consultation on Approaches to Managing Personal Data in the Digital Economy, the PDPC has proposed two new bases for organisations to collect, use or disclose personal data without the need for consent; namely, ‘notification of purpose’ and ‘legitimate interests’.

First, the PDPC has proposed to introduce ‘notification of purpose’ as a basis to collect, use or disclose personal data under the PDPA.
without consent, where the collection, use or disclosure of personal data is not expected to have any adverse impact on the individual. Organisations that wish to rely on this ‘legitimate interests’ basis must conduct a risk and impact assessment, such as a data protection impact assessment, as an accountability measure to identify and mitigate any risks when seeking to rely on the ‘notification of purpose’ basis.

Second, the PDPC has proposed to enable organisations to collect, use or disclose personal data without consent in circumstances where there is a need to protect legitimate interests that will have economic, social, security or other benefits for the public (or a section thereof). Such benefits to the public must outweigh any adverse impact to the individual, and organisations wishing to rely on this ‘legitimate interests’ basis must conduct a risk and impact assessment to determine this is the case. An additional safeguard, the PDPC intends to provide for an openness requirement whereby organisations relying on ‘legitimate interests’ as a basis to collect, use or disclose personal data must:
- disclose its reliance on ‘legitimate interests’ as a ground for collection, use or disclosure (eg, through the organisation’s data protection policy that is made available to the public); and
- make available a document justifying the organisation’s reliance on ‘legitimate interests’ and the business contact information of the person who is able to answer individuals’ questions about such collection, use or disclosure on behalf of the organisation.

The PDPC published its response to the public consultation on 1 February 2018, and it is expected that the proposed changes will be implemented in due course.

12 Legitimate processing – types of PII

Does the law impose more stringent rules for specific types of PII?

Generally, the PDPA does not distinguish between the types and sensitivities of personal data. However, section 24 of the PDPA requires that an organisation would need to make ‘reasonable security arrangements’ to protect, and to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks to personal data in its possession or under its control. The PDPC has noted that organisations should take into account the sensitivity of personal data when deciding on the appropriate level of security arrangements needed to protect it (see question 20).

Certain types of personal data are also accorded less stringent rules under the PDPA. For instance, the data protection provisions under the PDPA do not apply to personal data that has been contained in a record that has been in existence for at least 100 years. In addition, personal data pertaining to deceased individuals is also excluded from most of the obligations under the PDPA. In relation to such data, organisations will be subject only to the requirements to make reasonable security arrangements for the protection of such data, and the requirements relating to disclosure of personal data. These reduced obligations will apply for 10 years from the deceased’s date of death. In this regard, an individual appointed under the deceased’s will to exercise such rights (or, if there is no such person, the deceased’s nearest relative) may exercise all or any of the following rights in relation to the protection of the deceased’s personal data:
- the right to give or withdraw any consent for the purposes of the PDPA;
- the right to commence a private civil action in respect of any loss or damage suffered from a contravention of any of the provisions under Parts IV to VI of the PDPA; and
- the right to bring a complaint under the PDPA.

While the PDPA does not distinguish between the treatment of personal data of minors and that of individuals above 21 years of age, the PDPC has, in its Selected Topics Guidelines, recommended that organisations take appropriate steps to ensure that a minor can effectively give consent on his or her own behalf, in light of the circumstances of the particular case including the impact on the minor in giving consent. In this regard, the PDPC has also indicated that it will adopt the practical rule of thumb that a minor who is at least 13 years of age would typically have sufficient understanding to be able to consent on his or her own behalf. However, where, for example, an organisation has reason to believe or it can be shown that a minor does not have sufficient understanding of the nature and consequences of giving consent, the organisation should obtain consent from an individual who is legally able to provide consent on the minor’s behalf (eg, his or her parent or other legal guardian).

Data handling responsibilities of owners of PII

13 Notification

Does the law require owners of PII to notify individuals whose PII they hold? What must the notice contain and when must it be provided?

The obligation to notify stems primarily from the process of seeking valid consent (see question 11). In particular, organisations are obliged to inform individuals of:
(i) the purposes for the collection, use or disclosure of his or her personal data, on or before collecting the personal data;
(ii) any other purpose for the use or disclosure of personal data that has not been notified to the individual under (i), before such use or disclosure of personal data; and
(iii) on request by the individual, the business contact information of a person who is able to answer the individual’s questions about the collection, use or disclosure of the personal data on behalf of the organisation.

Only after the above information has been notified to the individual can he or she be considered to have validly given his or her consent to the collection, use or disclosure of his or her personal data in accordance with the purposes made known to him or her.

While the PDPA requires that such notice be provided to the individual on or before the collection, use and disclosure of his or her personal data, there is no prescribed manner or form in which such a notice must be given.

In relation to personal data that was collected by an organisation prior to the data protection provisions under the PDPA coming into effect on 2 July 2014, there is no express requirement under the PDPA that requires the organisation to notify individuals whose personal data they hold. However, fresh consent would need to be obtained from the individual concerned where the personal data collected is to be used for a different purpose from that to which consent was originally given. It follows that notification of the new purposes for which the personal data is to be collected, used or disclosed would also be required.

14 Exemption from notification

When is notice not required?

In addition, the Second, Third and Fourth Schedules to the PDPA also set out respectively certain circumstances where an individual’s consent need not be obtained for the collection, use and disclosure of his or her personal data (see question 11 for more details). Accordingly, the notification obligation would not apply under such circumstances.

However, section 20(4) of the PDPA carves out an exception to this concession. An organisation, on or before collecting, using or disclosing the personal data about an individual for the purpose of managing or terminating an employment relationship, has the obligation to inform the individual of that purpose, and, on request by the individual, the business contact information of a person who is able to answer the individual’s questions about the collection, use and disclosure on behalf of the organisation. This is despite the fact that the same organisation has no obligation to seek the consent of the individual before collecting, using or disclosing personal data for such purposes.

15 Control of use

Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

There is no specific requirement under the PDPA that compels organisations that hold the personal data of individuals to offer such individuals the right to have a degree of choice or control over the use of their personal data.
However, individuals have a right under section 16 of the PDPA to withdraw consent (including deemed consent) given to an organisation in respect of the collection, use or disclosure by that organisation of personal data about the individual for any purpose. The individual would need to give reasonable notice to the organisation as to the withdrawal of his or her consent. Thereafter, upon receipt of such notice, the organisation would need to inform the individual of the likely consequences of the withdrawal of consent, although the organisation should not prohibit the individual from withdrawing consent. Where the individual has withdrawn his or her consent, organisations would be required to inform their data intermediaries and agents to similarly cease collecting, using or disclosing the personal data of this individual.

16 Data accuracy
Does the law impose standards in relation to the quality, currency and accuracy of PII?
Section 23 of the PDPA generally requires that organisations make a reasonable effort to ensure that the personal data they collect is accurate and complete, if the personal data is likely to be used by the organisation to make a decision that affects the individual or is likely to be disclosed by the organisation to another organisation. This is regardless of whether the personal data is collected directly by the organisation or on behalf of the organisation.

The PDPC, in its Key Concepts Guidelines, has stated that an organisation must make a reasonable effort to ensure that:
- it accurately records the personal data it collects (whether directly from the individual concerned or through another organisation);
- the personal data it collects includes all relevant parts thereof (so that it is complete);
- it has taken the appropriate (reasonable) steps in the circumstances to ensure the accuracy and correctness of the personal data; and
- it has considered whether it is necessary to update the information.

The Key Concepts Guidelines also state that organisations, in deciding what is considered a reasonable effort, should take into account the following factors:
- the nature of the data and its significance to the individual concerned (eg, whether the data relates to an important aspect of the individual such as his or her health);
- the purpose for which the data is collected, used or disclosed;
- the reliability of the data (eg, whether it was obtained from a reliable source or through reliable means);
- the currency of the data (that is, whether the data is recent or was first collected some time ago); and
- the impact on the individual concerned if the personal data is inaccurate or incomplete (eg, based on how the data will be used by the organisation or another organisation to which the first organisation will disclose the data).

17 Amount and duration of data holding
Does the law restrict the amount of PII that may be held or the length of time it may be held?
Yes, section 25 of the PDPA provides that organisations (including data intermediaries) should cease to retain personal data, or remove the means by which it can be associated with particular individuals, as soon as it is reasonable to assume that:
- such retention no longer serves the purposes for which the data was collected; and
- retention is no longer necessary for legal or business purposes. Such legal or business purposes may, for example, include situations where the personal data is required for an ongoing legal action involving the organisation; where retention of the personal data is necessary in order to comply with the organisation’s obligations under other applicable laws; or where the personal data is required for an organisation to carry out its business operations, such as to generate annual reports or performance forecasts.

In addition, the PDPC in its Key Concepts Guidelines has clarified that personal data should not be kept by an organisation ‘just in case’ it may be needed. However, personal data may be retained so long as one or more of the purposes for which it was collected remains valid.

18 Finality principle
Are the purposes for which PII can be used by owners restricted? Has the ‘finality principle’ been adopted?
Yes, the purposes for which personal data can be used or disclosed by organisations is restricted to the purposes for which the individual concerned had given his or her consent to the organisation in respect of the same.

19 Use for new purposes
If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?
Generally, fresh consent would need to be obtained where organisations are seeking to collect, use or disclose personal data for different purposes from those to which the individual concerned had given his or her consent (see question 11).

Security
20 Security obligations
What security obligations are imposed on PII owners and service providers that process PII on their behalf?
Section 24 of the PDPA requires that organisations make ‘reasonable security arrangements’ to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. Organisations that process personal data on behalf of an organisation (ie, data intermediaries) are also subject to the same requirement. While the PDPC has recognised that there is no one-size-fits-all solution, it has, in its Key Concepts Guidelines, noted that an organisation should:
- design and organise its security arrangements to fit the nature of the personal data held by the organisation and the possible harm that might result from a security breach;
- identify reliable and well-trained personnel responsible for ensuring information security;
- implement robust policies and procedures for ensuring appropriate levels of security for personal data of varying levels of sensitivity; and
- be prepared and able to respond to information security breaches promptly and effectively.

In this regard, the PDPC has also published the following guidance documents to aid organisations in the management of electronic personal data and data breaches respectively:
- Guide to Securing Personal Data in Electronic Medium (Electronic Data Guide); and

The Electronic Data Guide sets out good infocommunications technology (ICT) security measures that organisations should adopt to protect electronic personal data (eg, in relation to ICT security audits and tests, authentication and authorisation, computer networks and email security); while the Data Breach Guide provides some guidance for organisations as to the effective management of data breaches.

21 Notification of data breach
Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?
There is presently no strict requirement prescribed under the PDPA to notify the PDPC or individuals of breaches of data security. However, in its Public Consultation on Approaches to Managing Personal Data in the Digital Economy, the PDPC has proposed a mandatory data breach notification requirement under the PDPA, to better oversee the level of incidences and management of data breaches at the national level. According to the PDPC’s responses to the public consultation (published 8 April 2018), the PDPC has proposed that organisations notify both the affected individuals and the PDPC in situations where the breach is ‘likely to result in significant harm or impact to the
individuals to whom the information relates. In contrast, where the breach does not pose any risk of impact or harm to affected individuals, but is of a significant scale (eg, 500 affected individuals), the PDPC has proposed that organisations notify the PDPC only if it learned of the breach and cooperated with the PDPC in its investigation.

In relation to the time-frame for notification, the PDPC has stated in its response that it intends to provide for an assessment period of up to 30 days from the day the organisation first becomes aware of a suspected data breach, to assess whether the suspected data breach is eligible for notification. Following the organisation’s assessment, where the organisation determines that the data breach is eligible for reporting, then the organisation must notify the relevant parties within the required time-frame (ie, ‘as soon as practicable’ to affected individuals, and ‘as soon as practicable, no later than 72 hours’ to the PDPC, from the time of determination). At the time of writing, the mandatory data breach notification requirement is not in effect yet, but is expected to be implemented in due course.

In addition to this, the Data Breach Guide states that it is good practice to notify individuals affected by a data breach, and that such notification should be given immediately if sensitive personal data is compromised. This is to allow such individuals to take necessary actions to prevent potential abuse of the compromised data.

Further, the Data Breach Guide recommends that organisations notify the PDPC as soon as possible of any data breach that might cause public concern or where there is a risk of harm to a group of affected individuals. Such notification should include the following information:

- the extent of the data breach;
- the type and volume of personal data involved;
- the cause or suspected cause of the breach;
- whether the breach has been rectified;
- the measures and processes that the organisation had put in place at the time of the breach;
- information on whether affected individuals were notified or when the organisation intends to do so; and
- contact details of persons with whom the PDPC may liaise for further information or clarification.

In this regard, the Data Breach Guide also states that whether organisations notify the PDPC of such data breaches, and whether they have adequate recovery procedures in place, will affect the PDPC’s decision on whether an organisation has reasonably protected the personal data under its control or possession.

In addition, one of the mitigating factors that the PDPC may consider when determining a financial penalty to be imposed on an organisation that has breached the PDPA, is whether the organisation voluntarily disclosed the personal data breach to the PDPC as soon as it learned of the breach and cooperated with the PDPC in its investigations (see question 4).

In addition, where criminal activity (eg, hacking, theft or unauthorised system access by an employee) is suspected, the Data Breach Guide also provides that the police should be notified.

**Internal controls**

**22 Data protection officer**

Is the appointment of a data protection officer mandatory?

What are the data protection officer’s legal responsibilities?

Yes, section 11 of the PDPA specifically requires that organisations designate one or more individuals to be the organisation’s data protection officer (DPO). This may be a person whose scope of work solely relates to data protection or a person in the organisation who takes on this role as one of his or her multiple responsibilities. The business contact information of at least one of these DPOs would need to be made known to the public.

The DPO is responsible for ensuring that the organisation complies with the provisions of the PDPA, although the designation of a DPO does not relieve an organisation of its obligations and liabilities (in the event of non-compliance with these obligations) under the PDPA.

The public guidance published on the PDPC’s website as of June 2018 sets out that the possible responsibilities of a DPO may include, but are not limited to, the following:

- ensuring compliance of the PDPA when developing and implementing policies and processes for handling personal data;
- fostering a data protection culture among employees and communicating personal data protection policies and processes to stakeholders;
- managing personal data protection-related queries and complaints;
- alerting the management to any risks that might arise with regard to personal data; and
- liaising with the PDPC on data protection matters, if necessary.

**23 Record keeping**

Are owners or processors of PII required to maintain any internal records or establish internal processes or documentation?

Yes, in order to be able to comply with access requests by individuals (see question 37), the Key Concepts Guidelines state that organisations are generally required to implement processes to keep track of the collection, use and disclosure of all personal data under their control, including unstructured data.

Organisations are also required under section 24 of the PDPA to make reasonable security arrangements to prevent the unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks to any personal data in their possession or under their control. While the PDPC has recognised that there is no one-size-fits-all solution for organisations, it has, in its Key Concepts Guidelines, noted that an organisation should:

- design and organise its security arrangements to fit the nature of the personal data held by the organisation and the possible harm that might result from a security breach;
- identify reliable and well-trained personnel responsible for ensuring information security;
- implement robust policies and procedures for ensuring appropriate levels of security for personal data of varying levels of sensitivity; and
- be prepared and able to respond to information security breaches promptly and effectively.

Organisations are also expected to cease retaining documents containing personal data, or remove the means by which personal data is associated with particular individuals, as soon as it is reasonable to assume that the purposes for which the personal data was collected is no longer being served by its retention, or the retention of the same is no longer necessary for legal or business purposes. The obligations above would apply to both the principal organisation and the data intermediary alike.

**24 New processing regulations**

Are there any obligations in relation to new processing operations?

There is presently no strict requirement prescribed under the PDPA for organisations to apply a privacy-by-design approach or carry out a privacy impact assessment. However, the DPIA Guide states that it is good practice for organisations to conduct regular Data Protection Impact Assessments (DPIAs) to assess and address personal data protection risks specific to the organisation. This would allow organisations to better assess their compliance with the PDPA, and thereupon implement appropriate operational or technical safeguards. The DPIA Guide describes the key aspects of a DPIA.

In brief, organisations should:

- provide an overview of the project and the key considerations surrounding the DPIA;
- define the scope of the DPIA, such as identifying the specific system or process that the DPIA needs to be carried out on;
- define the risk assessment framework or methodology for the DPIA;
- identify the parties whose inputs or views would have to be sought during consultation or interview sessions; and
- provide an estimate of time required for key tasks and overall timeline for conducting the DPIA.
Registration and notification

25 Registration

Are PII owners or processors of PII required to register with the supervisory authority? Are there any exemptions?

No, there is presently no such requirement under the PDPA for organisations that collect, use or disclose personal data (whether in the capacity of a principal organisation or a data intermediary) to register with the PDPC.

However, individuals may register their Singapore telephone numbers on one of the three DNC registers (for faxes, voice calls and text messages, including SMS or MMS messages, and any data applications that use a Singapore telephone number such as WhatsApp, iMessage or Viber). Individuals and organisations intending to make tele-marketing calls or send telemarketing messages (collectively referred to as specified messages) are required to check the relevant DNC registers within 30 days before sending such messages to ensure that recipient telephone numbers have not been registered before sending such specified messages.

26 Formalities

What are the formalities for registration?

There is presently no requirement under the PDPA for organisations to register with the PDPC.

With regard to the formalities for registration of Singapore telephone numbers on the DNC registers, as express registration is no longer offered from 23 May 2016, individuals may apply to add or remove their Singapore telephone number to or from the registers by any one of three methods:

- by calling a toll-free number to access the automated Interactive Voice Response System (IVRS), which will provide step-by-step instructions;
- by sending a text message to a designated number; or
- by registering online through the DNC registry website.

The registration of a Singapore telephone number on the DNC registry is free of charge and permanent until withdrawn by the user or subscriber, or until the relevant telecommunications service linked to the number is terminated.

27 Penalties

What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

There is presently no requirement under the PDPA for organisations to register with the PDPC.

However, organisations that make telemarketing calls or send specified messages are required to check the DNC registers regularly to ensure that recipient telephone numbers have not been registered on the relevant register, unless they have obtained clear and unambiguous consent in evidential form from the recipients. Failing to do so would be a contravention of the DNC registry rules under the PDPA, and would amount to an offence for which a fine of up to S$10,000 may be imposed.

28 Refusal of registration

On what grounds may the supervisory authority refuse to allow an entry on the register?

There is presently no requirement under the PDPA for organisations to register with the PDPC.

As for the DNC registry, only Singapore telephone numbers may be registered. Thus, non-Singapore telephone numbers cannot be registered on any of the DNC registers.

29 Public access

Is the register publicly available? How can it be accessed?

There is presently no requirement under the PDPA for organisations to register with the PDPC.

Organisations that send specified messages are required, within 30 days before sending such messages, to check the DNC registry before sending any such messages.

To access the DNC registry to perform such checks against the DNC registers, organisations are required to apply for an online account through the DNC registry website. This is a one-time application that results in the creation of a main account for the organisation. Main account holders can create as many sub-accounts as required. Creation of an account is open to organisations registered in Singapore, overseas organisations, and individuals (eg, freelancers and agents who conduct telemarketing activities). Fees are payable for creating main and sub-accounts, as well as for running checks on the DNC registry.

An account holder pays one ‘credit’ (or one to two cents, depending on the pre-paid credit package) for each phone number that is checked. From 1 June 2015, each main account receives 1,000 free credits every year (up from 500 free credits previously), which are valid for one year from the date the free credits are given, as a measure to help organisations, especially small and medium-size enterprises, comply with the DNC provisions by slightly defraying the costs of running such checks on the DNC registry.

30 Effect of registration

Does an entry on the register have any specific legal effect?

There is presently no requirement under the PDPA for organisations to register with the PDPC.

Individuals who register their Singapore telephone numbers on the DNC registry can expect to stop receiving unsolicited tele-marketing messages on their registered telephone numbers 30 days after registration.

31 Other transparency duties

Are there any other public transparency duties?

While there is no obligation on an organisation to make public statements on the nature of its processing of personal data per se, section 12 of the PDPA (also known as the Openness Obligation) requires an organisation to develop and implement policies and practices that are necessary for the organisation to meet its obligations under the PDPA, and to make such policies and practices known to the public.

As part of the Openness Obligation, an organisation is required to appoint a DPO and make available his or her contact details to the public. As good practice, the business contact information of the DPO should be readily accessible from Singapore, operational during Singapore business hours and, in the case of telephone numbers, be Singapore telephone numbers (see question 22).

For completeness, an organisation is also required under section 21 of the PDPA to provide individuals with the following information upon request:

- personal data that is in the possession or under the control of the organisation; and
- information about the ways in which that personal data has been or may have been used or disclosed within a year before the date of request for access (see question 27).

32 Transfer of PII

How does the law regulate the transfer of PII to entities that provide outsourced processing services?

Organisations that process personal data on behalf of another organisation (the principal organisation) are considered ‘data intermediaries’ under the PDPA. Such data intermediaries are exempt from most of the main data protection provisions under the PDPA. Data intermediaries are subject only to the data protection provisions relating to the protection and retention of personal data. Specifically, they are required to:

- make reasonable security arrangements to protect personal data in their possession or under their control in order to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks; and
- anonymise or cease retaining personal data, as soon as it is reasonable to assume that such retention no longer serves the purposes for which the data was collected, and retention is no longer necessary for legal or business purposes.
The principal organisation is subject to the full suite of data protection obligations under the PDPA as if it were processing the personal data itself.

33 Restrictions on disclosure
Describe any specific restrictions on the disclosure of PII to other recipients.

Disclosure of personal data to other recipients must be in accordance with the applicable requirements under the PDPA (see questions 11 and 13). Furthermore, in certain circumstances the PDPA restricts an organisation from providing an individual with:

- his or her personal data that is in the possession or under the control of the organisation; or
- information about the ways in which his or her personal data has been or may have been used or disclosed by the organisation within a year before the date of the request, in the situation where an individual has requested access to such personal data or information pursuant to the PDPA. See question 37 for a list of circumstances under which an individual’s right to access his or her personal data is restricted.

34 Cross-border transfer
Is the transfer of PII outside the jurisdiction restricted?

Yes, section 26 of the PDPA prohibits organisations from transferring personal data out of Singapore except in accordance with requirements prescribed under the PDPA to ensure that organisations provide a standard of protection to the transferred personal data that is comparable to the protection under the PDPA.

Under the PDP Regulations, all organisations transferring personal data from Singapore to countries or territories outside of Singapore are required to ensure that the recipient of such personal data is bound by ‘legally enforceable obligations’ to provide to the transferred personal data a standard of protection that is at least comparable to the protection accorded under the PDPA. These ‘legally binding obligations’ include obligations imposed under law, contract, binding corporate rules (for transfers to ‘related’ organisations), or any other legally binding instrument.

Where the transfer of personal data is pursuant to a contract, contractual clauses are to be contained in a legally binding contract that is enforceable against every receiving organisation under the contract. Such a contract must:

- require the recipient to provide a standard of protection for the personal data transferred to the recipient that is at least comparable to the protection under the PDPA; and
- specify the countries and territories to which the personal data may be transferred under the contract.

Where binding corporate rules are used, these rules must:

- require every related recipient of the transferred personal data to provide a standard of protection for the personal data transferred that is at least comparable to the protection under the PDPA; and
- specify:
  - the recipients of the transferred personal data to which the binding corporate rules apply;
  - the countries and territories to which the personal data may be transferred under the binding corporate rules; and
  - the rights and obligations provided by the binding corporate rules; and
- only be used for recipients that are related to the transferring organisation.

Notwithstanding, a transferring organisation is taken to have satisfied its obligation to ensure that the recipient is bound by legally enforceable obligations to provide to the transferred personal data a PDPA-comparable standard of protection, where:

- the individual consents to the transfer of the personal data to that recipient in that country or territory, after being provided with a reasonable summary in writing of the extent to which the personal data to be transferred will be protected to a PDPA-comparable standard, provided:
  - such consent was not required by the transferring organisation as a condition of providing a product or service, unless the transfer is reasonably necessary to provide the product or service to the individual; and
  - the transferring organisation did not obtain or attempt to obtain such consent by providing false or misleading information about the transfer, or by using other deceptive or misleading practices;
  - the transfer of the personal data to the recipient is necessary for the performance of a contract between the individual and the transferring organisation, or to do anything at the individual’s request with a view to the individual entering into a contract with the transferring organisation;
  - the transfer of the personal data to the recipient is necessary for the conclusion or performance of a contract between the transferring organisation and a third party that is entered into at the individual’s request;
  - the transfer of the personal data to the recipient is necessary for the conclusion or performance of a contract between the transferring organisation and a third party if a reasonable person would consider the contract to be in the individual’s interest;
  - the transfer of the personal data to the recipient is necessary for the personal data to be used:
    - for any purpose that is clearly in the interests of the individual (if consent for its use cannot be obtained in a timely way or the individual would not reasonably be expected to withhold consent);
    - to respond to an emergency that threatens the life, health or safety of the individual or another individual; or
    - in the national interest;
  - the transfer of the personal data to the recipient is necessary for the personal data to be disclosed:
    - for any purpose that is clearly in the interests of the individual, if consent for its disclosure cannot be obtained in a timely way;
    - to respond to an emergency that threatens the life, health or safety of the individual or another individual; or
    - where there are reasonable grounds to believe that the health or safety of the individual or another individual will be seriously affected and consent for the disclosure of the data cannot be obtained in a timely way (provided that the transferring organisation notifies the individual whose personal data is disclosed of such disclosure and the purposes for such disclosure, as soon as may be reasonably practicable);
    - in the national interest; or
    - for the purpose of contacting the next of kin or a friend of any injured, ill or deceased individual;
    - the personal data is in transit (ie, personal data transferred through Singapore in the course of onward transportation to a country or territory outside Singapore, without the personal data being accessed, used by or disclosed to any organisation (other than the transferring organisation or an employee of the transferring organisation) while the personal data is in Singapore, except for the purpose of such transportation); or
  - the personal data is publicly available in Singapore.

35 Notification of cross-border transfer
Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

No, there is presently no such requirement under the PDPA to notify the PDPC of transfers of personal data.

36 Further transfer
If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

The PDPA imposes an obligation on organisations transferring personal data out of Singapore to ensure that the recipient of such personal data is bound by ‘legally enforceable obligations’ to provide to the transferred personal data a standard of protection that is at least comparable to the protection accorded under the PDPA (see question 34). Where organisations use contractual clauses for the purpose of
imposing such ‘legally enforceable obligations’, the PDPC, in its Key Concepts Guidelines, distinguishes between data intermediaries and all other organisations (see questions 10 and 32 for more information on data intermediaries).

Where the recipient is a data intermediary, the transferring organisation has to set out minimal protections with regard to the protection and retention limitation of the personal data.

Where the recipient is an organisation other than a data intermediary, the transferring organisation has to set out protections for the transferred personal data with regard to:

- the purpose of collection, use and disclosure by the recipient;
- accuracy;
- protection;
- retention limitation;
- policies on personal data protection;
- access; and
- correction.

The PDPA does not explicitly require transferring organisations to ensure that the ‘legally enforceable obligations’ imposed on recipients apply to onward transfers of personal data to third-party organisations. However, to the extent that recipients are bound by legally enforceable obligations to provide a PDPA-comparable standard of protection in respect of the transferred personal data, recipients would similarly be obliged to ensure that any onward transfers of personal data are conducted in accordance with the requirements of the PDPA.

Rights of individuals

37 Access

Do individuals have the right to access their personal information held by PII owners? Describe how this right can be exercised as well as any limitations to this right.

Yes, under section 21 of the PDPA, individuals have the right to request an organisation to provide them with:

- their personal data that is in the possession or under the control of the organisation; and
- information about the ways in which that personal data has been or may have been used or disclosed within a year before the date of request for access.

This individual’s right of access is subject to a number of exceptions. Organisations are not allowed to provide an individual with his or her personal data or other information where such provision could reasonably be expected to:

- threaten the safety or physical or mental health of an individual other than the individual who made the request;
- cause immediate or grave harm to the safety or to the physical or mental health of the individual who made the request;
- reveal personal data about another individual;
- reveal the identity of an individual who has provided personal data about another individual and the individual providing the personal data does not consent to the disclosure of his or her identity; or
- be contrary to the national interest.

Further, the Fifth Schedule to the PDPA sets out certain situations where organisations are not required to accede to such requests. For example, organisations need not provide access to personal data or information as to how the personal data has been or may have been used or disclosed, in respect of:

- documents relating to a prosecution, if all proceedings related to the prosecution have not been completed;
- personal data that is subject to legal privilege;
- personal data that, if disclosed, would reveal confidential commercial information that could, in the opinion of a reasonable person, harm the competitive position of the organisation;
- personal data collected, used or disclosed without consent for the purposes of an investigation if the investigation and associated proceedings and appeals have not been completed; or
- any request:
  - that would unreasonably interfere with the operations of the organisation because of the repetitious or systematic nature of the requests;
  - if the burden or expense of providing access would be unreasonable to the organisation or disproportionate to the individual’s interests;
  - for information that does not exist or cannot be found;
  - for information that is trivial; or
  - that is otherwise frivolous or vexatious.

In addition, an organisation must not inform an individual that it has disclosed his or her personal data without his or her consent pursuant to certain exceptions under the Fourth Schedule to the PDPA, namely where:

- the disclosure is necessary for any investigation or proceedings; or
- the personal data is disclosed to any duly authorised officer of a prescribed law enforcement agency.

Under the PDP Regulations, organisations are entitled to charge the individual a reasonable fee for access to his or her personal data. This is to allow organisations to recover the incremental costs incurred in the form of time and effort spent by the organisation in responding to the access request. Under the PDPA, organisations are also required to respond to an access request as soon as reasonably possible. Subject to this, the PDP Regulations provide that, if an organisation is unable to respond to an access request within 30 days from the request, it must inform the individual in writing within that same time frame of the time by which it will be able to respond to the request (which should be the soonest possible time it can provide access).

In a situation where two or more individuals make an access request at the same time for their respective personal data captured in the same records, the Key Concepts Guidelines provide that:

- the organisation is required to provide each individual with access only to his or her own data unless consent from the other parties is obtained; and
- the prohibition under section 21(3)(c) of the PDPA does not apply where the other individual has consented to the disclosure of his or her personal data, or where any of the exceptions listed under the Fourth Schedule of the PDPA may apply.

The Key Concepts Guidelines further provide that:

- if an organisation is able to provide an individual with his or her personal data and other information without the personal data or other information excluded under sections 21(2), (3) and (4) of the PDPA, then an organisation must do so; and
- if an organisation has scheduled a periodic disposal of personal data, but has received an access request prior to such disposal, then it should identify such requested personal data as soon as reasonably possible and preserve the personal data while the access request is being processed.

In addition, the Access Requests Guide recommends, among other things, that:

- organisations should clearly make access request channels available (eg, access requests may be submitted in person, through email or by post);
- organisations should keep a record of all access requests received and processed, documenting clearly whether the requested access was provided or rejected, the rationale being that such proper documentation may help organisations in the event of a dispute or an application to the PDPC for a review;
- organisations should implement appropriate retention policies for the keeping of such records (ie, organisations should cease to retain records containing the individual’s personal data where retention is no longer necessary for any legal or business purposes); and
- organisations should preserve the personal data requested while processing an access request; for a duration of minimally 30 days after rejecting an access request; and for the whole duration when the PDPC is conducting a review of an organisation’s rejection of the access request and until any right of an individual for reconsideration and appeal is exhausted.
38 Other rights

Do individuals have other substantive rights?

Yes, section 22 of the PDPA provides an individual with the right to request an organisation to correct any error or omission in his or her personal data that is in the possession of or under the control of the organisation. This is, however, subject to certain exemptions. For instance, organisations need not correct any error or omission in any personal data about the individual that is in the possession or under the control of the organisation, upon request by the individual concerned, if the request relates to:

- opinion data kept solely by the organisation for an evaluative purpose;
- any examination conducted by an education institution, examination scripts and, prior to the release of examination results, examination results;
- personal data of the beneficiaries of a private trust kept solely for the purpose of administering the trust;
- personal data kept by an arbitral institution or a mediation centre solely for the purposes of arbitration or mediation proceedings administered by the arbitral institution or mediation centre; or
- a document related to a prosecution if all proceedings related to the prosecution have not been completed.

Unlike access requests, organisations are not entitled to charge a fee for correction requests. Under the PDPA, organisations are required to correct the personal data as soon as reasonably practicable. Subject to this, the PDP Regulations provide that, if an organisation is unable to make the necessary correction within 30 days from the request, it is required to inform the individual in writing within the same time frame of the time by which it will be able to do so (which should be the soonest practicable time it can make the correction). Unless it is satisfied on reasonable grounds that a correction should not be made, an organisation is required to correct the personal data, and send the corrected personal data to every organisation to which the personal data was disclosed within one year of the date the amendment was made, insofar as that organisation needs the corrected personal data for any legal or business purpose.

The PDPA also provides an individual with the right to commence a private action against an organisation where such an individual has suffered loss or damage directly as a result of non-compliance by the organisation of the data protection provisions under Parts IV to VI of the PDPA, subject to certain limitations (see question 39).

39 Compensation

Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Yes, any person who suffers loss or damage directly as a result of non-compliance by an organisation with the data protection provisions under Parts IV to VI of the PDPA will have a right of action for relief in civil proceedings in a court. However, where the PDPC has made a decision under the PDPA in respect of such a contravention, this right is only exercisable after such a decision issued by the PDPC becomes final after all avenues of appeal have been exhausted. The court may grant relief as it thinks fit, including an award of an injunction or declaration, or damages.

40 Enforcement

Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

The right to commence a private action for loss or damage suffered directly as a result of an organisation’s non-compliance with the PDPA would be an action for relief in civil proceedings. As mentioned, however, such right is only exercisable provided that any relevant infringement decision issued by the PDPC has become final after all avenues of appeal have been exhausted.

Therefore, if an individual becomes aware that an organisation has failed to comply with the PDPA, such individual may lodge a complaint to the organisation directly, or bring a complaint to the PDPC. Upon receipt of a complaint, the PDPC may then investigate or review the matter, or direct the parties as to the appropriate mode of dispute resolution.

Where the PDPC is satisfied that an organisation has breached the data protection provisions under the PDPA, the PDPC is empowered with a wide discretion to issue such remedial directions as it thinks fit. These include directions requiring the organisation to:

- stop collecting, using or disclosing personal data in contravention of the PDPA;
- destroy personal data collected in contravention of the PDPA;
- provide access to or correct personal data; or
- pay a financial penalty of up to S$1 million.

Should any organisation or individual be aggrieved by the PDPC’s decision or direction, such organisation or individual may request the PDPC to reconsider its decision or direction. Thereafter, any organisation or individual aggrieved by the PDPC’s reconsideration decision may submit an appeal to the Data Protection Appeal Panel. Alternatively, an aggrieved organisation or individual may appeal directly to the Data Protection Appeal Panel without first submitting a reconsideration request. An appeal can be made against the Data Protection Appeal Panel’s decision to the High Court on limited grounds, namely on a point of law or where such decision relates to the amount of a financial penalty. Reconsideration applications and appeal requests must be made within 28 days after the issuance of the relevant direction or decision; there is no automatic suspension of the direction or decision concerned except in the case of the imposition of a financial penalty or the amount thereof.

Exemptions, derogations and restrictions

41 Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

The application of the data protection provisions does not extend to ‘business contact information’, which is defined as ‘an individual’s name, position name or title, business telephone number, business address, business electronic mail address or business fax number and other similar information about the individual, not provided by the individual solely for his personal purposes’.

In addition, organisations are allowed to continue using (which could include disclosure that is necessarily part of such use) personal data collected before 2 July 2014, for the purposes for which the personal data was collected, unless consent for such use is withdrawn or the individual indicates or has indicated to the organisation that he or she does not consent to the use or disclosure of the personal data. In relation to the DNC provisions, the following messages are excluded from the meaning of a specified message under the Eighth Schedule to the PDPA and therefore not subject to the application of the DNC provisions:

- any message sent by a public agency under, or to promote, any programme carried out by any public agency that is not for a commercial purpose;
- any message sent by an individual acting in a personal or domestic capacity;
- any message that is necessary to respond to an emergency that threatens the life, health or safety of any individual;
- any message the sole purpose of which is:
  - to facilitate, complete or confirm a transaction that the recipient has previously agreed to enter into with the sender;
  - to provide warranty information, product recall information or safety or security information with respect to a product or service purchased or used by the recipient; or
  - to deliver goods or services, including product updates or upgrades, that the recipient is entitled to receive under the terms of a transaction that the recipient has previously agreed to enter into with the sender;
  - any message in relation to a subscription, membership, account, loan or comparable ongoing commercial relationship involving the ongoing purchase or use by the recipient of goods or services offered by the sender, the sole purpose of which is to provide:
    - notification concerning a change in the terms or features;
Update and trends

PDPC Public Consultation on Approaches to Managing Personal Data in the Digital Economy
There have been rapid developments in Singapore’s digital space, with the growth of Internet of Things devices, machine learning and artificial intelligence, as well as developments in the spheres of cloud computing and e-commerce. Data is an integral part of the digital economy, and as society becomes increasingly digitalised, the risk, scale and impact of data breaches will also increase. Cross-border data flows, whether within ASEAN or beyond the region, have also become the norm for a large majority of businesses with a presence in Singapore.

With the fast emergence of the digital economy, the PDPC has taken steps to review the PDPA as part of two public consultations, the Public Consultation for Approaches to Managing Personal Data in the Digital Economy (issued 27 July 2017), and the Public Consultation for Managing Unsolicited Commercial Messages and the Provision of Guidance to Support Innovation in the Digital Economy (issued 27 April 2018). While none of the proposed changes has been implemented, it is likely that the data privacy landscape in Singapore will change in tune with the digital economy, and developments in this sphere should be closely monitored.

- notification of a change in the standing or status of the recipient; or
- at regular periodic intervals, account balance information or other type of account statement;
- any message the sole purpose of which is to conduct market research or market survey; and
- any message sent to an organisation other than an individual acting in a personal or domestic capacity for any purpose of the receiving organisation.

In addition, the Personal Data Protection (Exemption from Section 43) Order 2013 exempts individuals and organisations sending specified messages to Singapore telephone numbers from the requirement to check the DNC registry, where they have an ongoing business relationship with the subscribers or users of those Singapore telephone numbers. However, the application of the exemption is subject to a number of conditions:
- at the time of the transmission of the specified message, the sender has to be in an ongoing relationship with the recipient;
- the purpose of the specified message has to be related to the subject of the ongoing relationship;
- only specified text and fax messages may be sent to the recipient.

Specific data processing

43 Internet use

Describe any rules on the use of ‘cookies’ or equivalent technology.

The PDPC has noted that any personal data collected through the use of ‘cookies’ would not be treated differently from other types of personal data, and organisations that collect personal data using cookies would equally be subject to the requirements of the PDPA. However, the Selected Topics Guidelines clarify that there may not be a need to seek consent for the use of cookies to collect, use or disclose personal data where the individual is aware of the purposes for such collection, use or disclosure and voluntarily provides his or her personal data for such purposes. Such activities include (but are not limited to) transmitting personal data for effecting online communications and storing information that the user enters in a web form to facilitate an online purchase. Further, for activities that cannot take place without cookies that collect, use or disclose personal data, consent may be deemed if the individual voluntarily provides the personal data for that purpose of the activity, and it is reasonable that he or she would do so. In situations where the individual configures his or her browser to accept certain cookies but rejects others, he or she may be deemed to have consented to the collection, use and disclosure of the personal data by the cookies that he or she has chosen to accept. However, the mere failure of an individual to actively manage his or her browser settings does not imply that he or she has consented to the collection, use and disclosure of personal data by all websites for their stated purpose.

In addition, the Selected Topics Guidelines make clear that where organisations use cookies for behavioural targeting that involves the collection and use of an individual’s personal data, the individual’s consent is required.

44 Electronic communications marketing

Describe any rules on marketing by email, fax or telephone.

Organisations that make telemarketing calls or send messages of a commercial nature are required to check the DNC registry at least once every 30 days before sending any such marketing messages, unless they have obtained clear and unambiguous consent from the recipients in evidential form. See question 29 for details on how checks on the DNC registry can be conducted.

Regarding the rules on marketing by email, the Spam Control Act governs the sending of unsolicited emails or spam in Singapore. For more details on the specifics of contravening these rules, see question 6.

As mentioned above, the PDPC is proposing to review, streamline and merge the DNC provisions of the PDPA and the Spam Control Act into a single legislation governing all unsolicited commercial messages, and is currently seeking comments on this as part of its Public Consultation for Managing Unsolicited Commercial Messages and the
Cloud services

Describe any rules or regulator guidance on the use of cloud computing services.

Generally, cloud computing service providers (CCSPs) are required to comply with the PDPA (in particular, the obligation to implement reasonable security arrangements to protect personal data in their possession or under their control); any applicable subsidiary legislation that may be enacted from time to time; and any applicable sector-specific data protection frameworks to the extent that CCSPs provide cloud services to customers operating in these sectors.

Notably, CCSPs are required to make reasonable security arrangements to protect personal data in their possession or under their control. While there is no one-size-fits-all approach in complying with this obligation, the guidance issued by the PDPC may be relevant in assessing whether a CCSP has fulfilled its obligation. For instance, the Data Breach Guide sets out broad steps that organisations may consider taking in planning for and responding to data breaches as well as the Electronic Data Guide, which sets out a good number of practices for organisations to take to protect electronic personal data.

In addition, while the following standards and guidelines are not legally binding per se, these standards and guidelines may also be relevant in assessing whether a CCSP has met the obligation to implement reasonable security arrangements to protect personal data in its possession or under its control under the PDPA:

- Multi-Tier Cloud Security Standard for Singapore 584, a set of security standards issued by the Singapore Information Technology (IT) Standards Committee for voluntary adoption by CCSPs, which provides for three tiers of security certification (tier 1 being the base level and tier 3 being the most stringent); and
- Cloud Outage Incident Response Guidelines (COIR), issued by the Info-communications Development Authority of Singapore (as the IMDA was previously known) on 26 February 2016 for voluntary adoption by CCSPs, guides CCSPs in planning for and responding to cloud outages. The main objective of the COIR is to provide a tiered framework for transparency in cloud service providers’ cloud outage incident response for cloud users. Under the COIR, cloud users would be able to opt for the appropriate tier of outage protection and data breaches notification so as to complement their own business continuity and IT disaster recovery capabilities, including fulfilling any legal and regulatory duties.