



Data Protection 2025

12th Edition



Contributing Editors:

Tim Hickman & Dr. Detlev Gabel

White & Case LLP

glg Global Legal Group

Expert Analysis Chapters

- 1** The Rapid Evolution of Data Protection Laws
Tim Hickman & Dr. Detlev Gabel, White & Case LLP
- 8** AI Regulatory Landscape and Development Trends in China
Kate Yin, Gil Zhang, Sherman Deng & Huihui Li, Fangda Partners
- 17** The Increased Relevance for Companies of Data Collection of Racial and Ethnic Origins in the EU
Pierre Affagard & Laure Ekani, Clyde & Co LLP
- 24** Cloud Computing, Privacy Impact Assessments and Record-Keeping Regarding Data Protection in Japan
Yusaku Akasaki, Hiroki Minekawa & Ronald Kaloostian, Chuo Sogo LPC

Q&A Chapters

- 29** **Australia**
Darren Pham, Phillip Salakas & Harry Sultan,
Nyman Gibson Miralis
- 47** **Brazil**
Larissa Galimberti, Luiza Fonseca de Araujo &
Cecília Alberton Coutinho Silva,
Pinheiro Neto Advogados
- 64** **China**
Susan Ning & Han Wu, King & Wood Mallesons
- 81** **Egypt**
Ibrahim Shehata, Tasneem ElNaggar & Safa Rabea,
Shehata & Partners
- 96** **France**
Clara Hainsdorf & Bertrand Liard,
White & Case LLP
- 107** **Germany**
Martin Röleke & Dr. Evelyne Sørensen,
activeMind.legal Rechtsanwalts-gesellschaft mbH
- 120** **Greece**
Dr. Nikos Th. Nikolinakos, Dina Th. Kouvelou &
Alexis N. Spyropoulos, Nikolinakos & Partners Law Firm
- 135** **Hungary**
Adam Liber & Tamás Bereczki,
BLB Legal – Bagdi-Liber-Bereczki Attorneys-at-Law
- 145** **India**
Rachit Bahl, Rohan Bagai, Sumit Ghoshal &
Archana Iyer, AZB & Partners
- 156** **Indonesia**
Abadi Abi Tisnadisastra, Prayoga Mokoginta &
Aloysius Andrew Jonathan,
ATD Law in association with Mori Hamada
- 167** **Ireland**
Victor Timon, Zelda Deasy, Seán O'Donnell &
Jane O'Grady, Byrne Wallace Shields LLP
- 181** **Isle of Man**
Caitlin Gelder, Kathryn Sharman & Sinead O'Connor,
DQ Advocates Limited
- 192** **Israel**
Vered Zlaikha, Ariella May & Shahar Talmon,
Lipa Meir & Co.
- 205** **Japan**
Hiromi Hayashi & Masaki Yukawa,
Mori Hamada & Matsumoto
- 219** **Mexico**
Abraham Diaz, Gustavo Alcocer & Carla Huitron,
OLIVARES
- 229** **Nigeria**
Jumoke Lambo, Chisom Okolie, Opeyemi Adeshina &
Joel Adeyemi Adefidipe, Udo Udoma & Belo-Osagie
- 245** **Pakistan**
Saifullah Khan & Saeed Hasan Khan,
S. U. Khan Associates Corporate & Legal Consultants
- 254** **Poland**
Jakub Gładkowski, Barbara Kieltyka &
Małgorzata Kieltyka, Kieltyka Gladkowski KG Legal
- 271** **Saudi Arabia**
Saifullah Khan & Saeed Hasan Khan,
Droua Al-Amal Consultants
- 282** **Serbia**
Vladimir Djerić, Lena Petrovic, Katarina Radovic &
Kristina Petronijevic, Mikijelj Jankovic & Bogdanovic
- 295** **Singapore**
Lim Chong Kin & Anastasia Su-Anne Chen,
Drew & Napier LLC
- 312** **Switzerland**
Daniela Fábíán, FABIAN PRIVACY LEGAL GmbH
- 322** **Taiwan**
Yvonne Y.F. Lin, Jeffrey K.S. Hung & Jackie Yang,
Formosan Brothers Attorneys-at-Law
- 331** **Ukraine**
Vladyslav Podolyak & Tetiana Partsei, Arriba
- 345** **United Arab Emirates**
Saifullah Khan & Saeed Hasan Khan,
Bizilance Legal Consultants
- 357** **United Kingdom**
Tim Hickman & Aishwarya Jha, White & Case LLP
- 370** **USA**
F. Paul Pittman, Abdul Hafiz & Andrew Hamm,
White & Case LLP

Singapore



Lim Chong Kin



Anastasia Su-Anne Chen

Drew & Napier LLC

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The Personal Data Protection Act 2012 (“**PDPA**”) is the principal data protection legislation in Singapore. The PDPA established a general data protection law which applies to all private-sector organisations.

In 2020, the PDPA underwent its first comprehensive review since its enactment. The amendments are set out in the Personal Data Protection (Amendment) Act 2020 (“**Amendment Act**”). The Amendment Act, which was passed in Parliament on 2 November 2020, sets out extensive amendments, which mostly came into effect on 1 February 2021.

Parts 3 to 6A of the PDPA set out obligations of organisations in respect of the collection, use, disclosure, access, correction, care, protection, retention, transfer of personal data and notification of data breaches (collectively, “**Data Protection Provisions**”); while Part 9 of the PDPA sets out provisions pertaining to Singapore’s national Do Not Call (“**DNC**”) Registry and the obligations of organisations in relation to sending marketing messages to Singapore telephone numbers (“**DNC Provisions**”).

Other regulations issued under the PDPA are:

- the Personal Data Protection Regulations 2021 (“**PDP Regulations**”), which set out the requirements for transfers of personal data out of Singapore; the form, manner and procedures for requests for access to or correction of personal data; and persons who may exercise rights in relation to disclosure of personal data of deceased individuals;
- the Personal Data Protection (Notification of Data Breaches) Regulations 2021 (“**Breach Notification Regulations**”);
- the Personal Data Protection (Composition of Offences) Regulations 2021;
- the Personal Data Protection (Do Not Call Registry) Regulations 2013;
- the Personal Data Protection (Enforcement) Regulations 2021; and
- the Personal Data Protection (Appeal) Regulations 2021.

In addition, the Personal Data Protection Commission (“**PDPC**”) has issued a number of advisory guidelines which provide greater clarity on the interpretation of the PDPA.

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

The Computer Misuse Act 1993 sets out a number of offences which include the unauthorised access or modification of computer material, as well as the unauthorised use or interception of computer services.

The Cybersecurity Act 2018 requires owners and operators of Critical Information Infrastructure to comply with cybersecurity policies and standards, conduct audits and risk assessments, and implement incident reporting measures.

For completeness, the Spam Control Act 2007 (“**SCA**”) regulates the bulk sending of unsolicited commercial electronic messages to email addresses or mobile telephone numbers, complementing the DNC Provisions of the PDPA.

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

Yes, a number of other regulations and pieces of legislation in Singapore contain certain sector-specific data protection requirements. For example:

- the Banking Act 1970 (“**Banking Act**”) contains a number of banking secrecy provisions which govern customer information obtained by banks;
- the Telecom and Media Competition Code 2022 issued under the Telecommunications Act 1999 contains provisions governing the use of end-user service information by telecoms licensees; and
- the Healthcare Services Act 2020 (No. 3 of 2020), which replaces the Private Hospitals and Medical Clinics Act (Cap 248), contains provisions relating to the confidentiality of information held by healthcare service providers licensed under the Act.

With regard to the financial sector, the Monetary Authority of Singapore (“**MAS**”) is empowered under the Monetary Authority of Singapore Act 1970 and other sectoral legislation to issue directives and notices. Examples of MAS-issued regulatory instruments which are relevant to data protection include the Notices on Cyber Hygiene, Notices and Guidelines on Technology Risk Management, and the Guidelines on Outsourcing.

In this regard, Section 4(6) of the PDPA provides that the general data protection framework does not affect any right or obligation under other written laws, and that in the event of any inconsistency, the provisions of other written laws will prevail.

The PDPC has also developed sector-specific advisory guidelines for the telecommunications sector, the real estate agency sector, the education sector, the healthcare sector, the social services sector and transport services for hire (specifically in relation to in-vehicle recordings).

In addition, the PDPC has provided comments and suggestions to industry-led guidelines on the PDPA that were developed by industry associations such as:

- the Life Insurance Association Singapore (“LIA”) Code of Practice for Life Insurers on the Singapore Personal Data Protection Act; and
- the LIA Code of Conduct for Tied Agents of Life Insurers on the Singapore Personal Data Protection Act.

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

The PDPC is responsible for administering and enforcing the PDPA. The PDPC is under the purview of the Ministry of Communications and Information (“MCI”), and is part of the merged info-communications and media regulator, the Info-communications Media Development Authority of Singapore (“IMDA”) (previously the Info-communications Development Authority of Singapore and the Media Development Authority of Singapore).

Sector-specific data protection obligations are separately enforced by the relevant sectoral regulators. For example, the MAS enforces the banking secrecy provisions under the Banking Act and other sectoral legislation and regulatory instruments governing other types of financial institutions.

2 Definitions

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

- **“Personal Data”**
“Personal data” is defined under the PDPA as data, whether true or not, about an individual who can be identified: (a) from that data; or (b) from that data and other information to which the organisation is likely to have access.
All formats of personal data are covered under the PDPA, whether electronic or non-electronic, and regardless of the degree of sensitivity.
- **“Processing”**
Under the PDPA, “processing”, in relation to personal data, means the carrying out of any operation or set of operations in relation to the personal data, and includes any of the following:
 - (a) recording;
 - (b) holding;
 - (c) organisation, adaptation or alteration;
 - (d) retrieval;
 - (e) combination;
 - (f) transmission; and
 - (g) erasure or destruction.
- **“Controller”**
The PDPA does not use the term “controller”, but instead refers to an “organisation”. An “organisation” is defined as any individual, company, association or body of persons, corporate or unincorporated, whether or not:
 - (a) formed or recognised under the law of Singapore; or
 - (b) resident, or having an office or a place of business, in Singapore.

- **“Processor”**
Similarly, the PDPA does not use the term “processor”, but instead refers to a “data intermediary”, which is defined as an organisation which processes personal data on behalf of another organisation but does not include an employee of that other organisation.
The PDPA provides that a data intermediary that processes personal data on behalf of and for the purposes of another organisation pursuant to a contract which is evidenced or made in writing will only be subject to (i) the Protection Obligation, (ii) the Retention Limitation Obligation (as defined below), and (iii) the requirement to notify the data controller without undue delay where the data intermediary has reason to believe that a data breach has occurred in relation to personal data that it is processing on the data controller’s behalf.
- **“Data Subject”**
The PDPA does not use the term “data subject”, but instead refers generally to an “individual”, whose personal data is collected, used, disclosed, or otherwise processed by organisations. An “individual” is defined to mean a natural person, whether living or deceased.
- **“Sensitive Personal Data”/“Special Categories of Personal Data”**
The PDPA does not expressly distinguish between specific categories of personal data. The term “sensitive personal data” is not defined.
However, as a number of the Data Protection Provisions adopt a standard of reasonableness, the sensitivity of the personal data in question could, in practice, affect the application of the data protection obligations. For example, the PDPC has taken the position in several enforcement decisions that a higher standard of protection is required for more sensitive personal data, which includes insurance, medical and financial data (see *In Re Aviva Ltd* [2017] SGPDP 14).
In this regard, the PDPC’s Advisory Guidelines on Enforcement for Data Protection Provisions (“**Enforcement Guidelines**”) provide that, if an organisation which has breached a Data Protection Provision is in the business of handling large volumes of sensitive personal data, the disclosure of which may cause exceptional damage, injury or hardship to a person (such as medical or financial data), but failed to put in place adequate safeguards proportional to the harm that might be caused by disclosure of such personal data, the PDPC may also consider this to be an aggravating factor in calculating the level of the financial penalty to be imposed on the organisation.
Additionally, in the Breach Notification Regulations, the PDPC prescribes a list of personal data that, if subject to a data breach, would be deemed to result in significant harm to individuals. These include the following broad categories of personal data:
 - (a) financial information which is not publicly disclosed;
 - (b) personal data which would lead to the identification of vulnerable individuals (e.g. leading to identification of a minor who has been arrested for an offence);
 - (c) life, accident and health insurance information which is not publicly disclosed;
 - (d) specified medical information, including the assessment and diagnosis of HIV infections;
 - (e) information related to adoption matters;
 - (f) a private key used to authenticate any or digitally sign an electronic record or transaction; and

(g) an individual's account identifier and data for access into the individual's account.

- **“Data Breach”**

“Data breach” is defined in Section 24 of the PDPA to mean: (a) the unauthorised access, collection, use, disclosure, copying, modification or disposal of personal data; or (b) the loss of any storage medium or device on which personal data is stored in circumstances where the unauthorised access, collection, use, disclosure, copying, modification or disposal of the personal data is likely to occur.

- **“Business Contact Information”**

“Business contact information” is defined in Section 2(1) of the PDPA to mean: an individual's name, position name or title, business telephone number, business address, business electronic mail address or business fax number and any other similar information about the individual, not provided by the individual solely for his or her personal purposes.

The Data Protection Provisions do not apply to “business contact information”.

3 Territorial and Material Scope

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

The PDPA applies to all organisations that are not a public agency, whether or not formed or recognised under the laws of Singapore, or resident or having an office or a place of business in Singapore.

According to the PDPC's Advisory Guidelines on Key Concepts in the PDPA (“**Key Concepts Guidelines**”), the Data Protection Provisions apply to organisations carrying out activities involving personal data in Singapore. Thus, where personal data is collected overseas and subsequently transferred into Singapore, the Data Protection Provisions will apply in respect of the activities involving the personal data in Singapore.

3.2 Do the data protection laws in your jurisdiction carve out certain processing activities from their material scope?

Yes. The Data Protection Provisions of the PDPA do not apply to individuals acting in a personal or domestic capacity. The PDPA also does not impose the Data Protection Provisions on an employee acting in the course of his employment within an organisation (Section 4(1)(a), (b) of the PDPA).

4 Key Principles

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

- **Transparency**

Section 20 of the PDPA provides that an organisation must notify an individual of the purpose(s) for which it intends to collect, use or disclose his personal data, on or before such collection, use, or disclosure (“**Notification Obligation**”).

More generally, Sections 11 and 12 of the PDPA require an organisation to develop and implement policies and practices that are necessary for the organisation to meet its obligations under the PDPA, communicate such policies and practices to its employees, and make information about its policies and procedures publicly available (“**Accountability Obligation**”). Accountability under the PDPA requires organisations to undertake measures in order to ensure that they meet their obligations under the PDPA and, importantly, demonstrate that they can do so when required. The Accountability Obligation also requires an organisation to appoint a Data Protection Officer (“**DPO**”) (see section 8 below).

- **Lawful basis for processing**

Sections 13 to 17 of the PDPA generally require that an organisation obtain the consent of an individual before collecting, using or disclosing his personal data for a purpose (“**Consent Obligation**”), unless an exception in the First or Second Schedule to the PDPA applies. Such consent from an individual must be validly obtained and may be either expressly given or deemed to have been given.

- **Purpose limitation**

Section 18 of the PDPA provides that an organisation may collect, use or disclose personal data about an individual only for purposes that a reasonable person would consider appropriate in the circumstances and, where applicable, if the individual concerned has been notified (“**Purpose Limitation Obligation**”).

- **Data minimisation**

The PDPA does not articulate the principle of data minimisation (i.e. the limitation of personal data collection to what is directly relevant and necessary to accomplish a specified purpose), although the Purpose Limitation Obligation and Retention Limitation Obligation (as defined below) operate to limit the collection, use, disclosure and retention of personal data by organisations to some extent.

Nonetheless, the PDPC recommends that organisations avoid the over-collection of personal data where this is not required for their business or legal purposes. Instead, the PDPC encourages organisations to consider whether there are alternative ways of addressing their requirements.

- **Proportionality**

While the PDPA does not explicitly refer to the principle of proportionality, a number of the Data Protection Provisions – for instance, the Purpose Limitation Obligation, the Accuracy Obligation, the Protection Obligation and the Retention Limitation Obligation (as defined below) – refer to a standard of reasonableness.

More generally, Section 11(1) of the PDPA states that an organisation shall, in meeting its responsibilities under the PDPA, “consider what a reasonable person would consider appropriate in the circumstances”.

In this regard, the PDPC's Key Concepts Guidelines state that a “reasonable person” is judged based on an objective standard and can be said to be a person who exercises the appropriate care and judgment in the particular circumstances.

- **Retention**

While the PDPA does not prescribe any specific data retention periods, Section 25 of the PDPA provides that an organisation must cease to retain documents containing personal data, or remove the means by which

the personal data can be associated with particular individuals as soon as it is reasonable to assume that (a) the purpose for which the personal data was collected is no longer being served by retention of the personal data, and (b) retention is no longer necessary for legal or business purposes (“**Retention Limitation Obligation**”).

- **Accuracy**

Section 23 of the PDPA requires an organisation to make a reasonable effort to ensure that personal data collected by or on behalf of the organisation is accurate and complete, if the personal data is likely to be used by the organisation to make a decision that affects the individual to whom the personal data relates, or is likely to be disclosed by the organisation to another organisation (“**Accuracy Obligation**”).

- **Protection**

Section 24 of the PDPA requires an organisation to make reasonable security arrangements to protect personal data in its possession or under its control, in order to prevent (i) unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks, and (ii) the loss of any storage medium or device on which personal data is stored. (“**Protection Obligation**”) (see our responses to section 16 below).

- **Transfer Limitation**

Section 26 of the PDPA provides that an organisation must not transfer any personal data to a country or territory outside Singapore, except in accordance with prescribed requirements to ensure that the overseas recipient provides a standard of protection to the transferred personal data that is comparable to the protection under the PDPA (“**Transfer Limitation Obligation**”) (see our responses to section 12 below).

5 Individual Rights

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

- **Right of access to (copies of) data/information about processing**

Under Section 21 of the PDPA, an individual has the right to request an organisation to allow him access to his personal data.

Specifically, unless a relevant exception under the PDPA applies, an organisation is required to, on request by an individual, provide him with: (a) his personal data in the possession or under the control of the organisation; and (b) information about the ways in which that personal data has been or may have been used or disclosed by the organisation within a year before the date of the individual’s request (“**Access Obligation**”).

There are a number of exceptions to the Access Obligation. Specifically, an organisation is not required to provide an individual with his personal data or other information, in respect of the matters specified under the Fifth Schedule to the PDPA, which include, without limitation:

- opinion data kept solely for an evaluative purpose;
- personal data which, if disclosed, would reveal confidential commercial information that could, in the opinion of a reasonable person, harm the competitive position of the organisation;
- personal data collected, used or disclosed without consent, for the purposes of an investigation if

the investigation and associated proceedings and appeals have not been completed; and

- any request:
 - that would unreasonably interfere with the operations of the organisation because of the repetitive or systematic nature of the requests;
 - where the burden or expense of providing access would be unreasonable to the organisation or disproportionate to the individual’s interests;
 - for information that does not exist or cannot be found;
 - for information that is trivial; or
 - that is otherwise frivolous or vexatious.

In addition, Section 21(3) of the PDPA provides that an organisation shall not provide an individual with his personal data or other information, if doing so could be reasonably expected to:

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

With respect to third-party personal data, certain exclusion(s) do not apply to any user activity data about, or any user-provided data from, the individual who made the request, despite such data containing personal data about another individual.

- **Right to rectification of errors**

Under Section 22 of the PDPA, an individual has the right to request that an organisation correct an error or omission in his personal data.

Specifically, an organisation is required to, on request by an individual: (a) correct an error or omission in the individual’s personal data that is in the possession or under the control of the organisation; and (b) send the corrected personal data to every other organisation to which the personal data was disclosed by the organisation within a year before the date the correction request was made, unless that other organisation does not need the corrected personal data for any legal or business purpose (“**Correction Obligation**”).

However, Section 22(7) of the PDPA provides that an organisation is not required to comply with the Correction Obligation in respect of the following matters specified in the Sixth Schedule to the PDPA:

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

In addition, Section 22(6) of the PDPA provides that an organisation is not required to correct or otherwise alter an opinion, including a professional or an expert opinion.

- **Right to deletion/right to be forgotten**
The PDPA does not accord an individual the right to require an organisation to delete his personal data.
- **Right to object to processing**
Under Section 16 of the PDPA, an individual may, upon giving reasonable notice to an organisation, withdraw his consent (which includes deemed consent) given to the organisation for the collection, use or disclosure of his personal data for any purpose. Upon withdrawal of consent, the organisation must cease (and cause its data intermediaries and agents to cease) collecting, using or disclosing the personal data, as the case may be, unless the collection, use or disclosure of the personal data without consent is required or authorised under the PDPA or any other written law.
- **Right to restrict processing**
Please see our response to “Right to object to processing” above.
- **Right to data portability**
The Amendment Act has introduced a Data Portability Obligation, which is set out in Part 6B of the PDPA. However, it has yet to come into effect. Broadly, the Data Portability Obligation provides that subject to certain exceptions and conditions, upon an organisation’s receipt of a data porting request from an individual, the porting organisation must transmit the applicable data specified in the data porting request to the receiving organisation in accordance with any prescribed requirements.
- **Right to withdraw consent**
Please see our response to “Right to object to processing” above.
- **Right to object to marketing**
Please see our response to “Right to object to processing” above.
In addition, an individual who does not wish to receive specified telemarketing calls and messages addressed to his Singapore telephone number may register his Singapore telephone number on one or more of the three DNC registers (namely, the No Voice Call Register; the No Text Message Register; and the No Fax Message Register) (see our response to question 10.1 below).
- **Right protecting against solely automated decision-making and profiling**
The PDPA does not accord an individual a right against solely automated decision-making and profiling. However, individuals may withdraw consent, if they oppose to automated decision-making and profiling conducted by organisations. Please see our response to “Right to object to processing” above.
- **Right to complain to the relevant data protection authority(ies)**
An individual may lodge a complaint with the PDPC in respect of an organisation’s breach of any of the Data Protection Provisions or DNC Provisions. Upon receiving such a complaint, the PDPC may: direct the individual and the organisation to resolve the complaint; refer the matter for mediation; or conduct an investigation to determine whether or not the organisation is in compliance with the PDPA.

5.2 Please confirm whether data subjects have the right to mandate not-for-profit organisations to seek remedies on their behalf or seek collective redress.

The PDPA does not accord individuals the right to mandate not-for-profit organisations to seek remedies on their behalf or seek collective redress.

However, Section 48O of the PDPA confers upon individuals who have suffered loss or damage directly as a result of a contravention of the provisions of the PDPA the right to commence a private civil action.

6 Children’s Personal Data

6.1 What additional obligations apply to the processing of children’s personal data?

There are no specific provisions in the PDPA regulating the processing of children’s data.

Nevertheless, in its Advisory Guidelines on the PDPA for Selected Topics, the PDPC has stated that organisations should generally consider whether a minor has sufficient understanding of the nature and consequences of giving consent in determining whether the minor can effectively provide consent on his own behalf of the purposes of the PDPA.

The PDPC has also stated that as a practical rule of thumb, a minor who is at least 13 years of age would typically have sufficient understanding to be able to consent on his own behalf. However, it also states that where 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, such as the minor’s parent or guardian.

On 28 March 2024, the PDPC published its Advisory Guidelines on the PDPA for Children’s Personal Data in the Digital Environment (“**Children’s Personal Data Guidelines**”). The Children’s Personal Data Guidelines apply to organisations whose online products or services are likely to be accessed by children.

The PDPC clarified that it considers that a child between 13 and 17 years old may give valid consent when the policies on the collection, use and disclosure of the child’s personal data, as well as the withdrawal of consent, are readily understandable to them. This includes ensuring that the child understands the consequences of providing and withdrawing his consent. If an organisation has reason to believe that a child does not have sufficient understanding of the nature and consequences of giving consent, the organisation should obtain consent from the parent or guardian.

The Children’s Personal Data Guidelines also state that the PDPC will consider the use of a child’s personal data or profile to target harmful or inappropriate content (as defined in the Code of Practice for Online Safety, issued under the Broadcasting Act 1994) as unreasonable. Additionally, children’s personal data are also to be generally considered as sensitive personal data and must be accorded a higher standard of protection under the PDPA.

Organisations are also advised to conduct data protection impact assessments before releasing products or services that are likely to be accessed by children in order to meet their Accountability Obligation under the PDPA.

7 Registration Formalities and Prior Approval

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

There is currently no requirement for organisations to register with or notify the PDPC.

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

This is not applicable in Singapore.

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

This is not applicable in Singapore.

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

This is not applicable in Singapore.

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

This is not applicable in Singapore.

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

This is not applicable in Singapore.

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

This is not applicable in Singapore.

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

This is not applicable in Singapore.

7.9 Is any prior approval required from the data protection regulator?

This is not applicable in Singapore.

7.10 Can the registration/notification be completed online?

This is not applicable in Singapore.

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

This is not applicable in Singapore.

7.12 How long does a typical registration/notification process take?

This is not applicable in Singapore.

8 Appointment of a Data Protection Officer

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

The appointment of a DPO is mandatory. Section 11(3) of the PDPA obliges an organisation to designate one or more individuals to be responsible for ensuring that the organisation complies with the PDPA.

The business contact information of at least one DPO must be made available to the public (e.g. email address or Singapore phone number) pursuant to Section 11(5) of the PDPA. This business contact information should be readily accessible from Singapore, operational during Singapore business hours and, in the case of telephone numbers, be Singapore telephone numbers. This is especially important if the DPO is not physically based in Singapore, as it would facilitate the organisation's ability to respond promptly to any complaint or query on its data protection policies and practices.

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

Generally, the PDPC may take the following enforcement actions against the organisation:

- (a) give the organisation such directions as the PDPC sees fit in the circumstances to ensure compliance; and/or
- (b) require the organisation to pay a financial penalty up to a maximum of 10% of the organisation's annual turnover in Singapore, or S\$1 million, whichever is higher.

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

The PDPA does not provide for any particular protections for DPOs in respect of their role as DPOs. However, to the extent that the DPO is an employee of the organisation, Section 4(1)(a) of the PDPA provides that the Data Protection Provisions do not apply to an employee acting in the course of his employment.

It should be noted that the appointment of a DPO does not relieve the organisation of its obligations and liabilities under the PDPA.

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

Yes. Section 11(3) of the PDPA only provides that each organisation “shall designate one or more individuals to be responsible for ensuring that the organisation complies with [the PDPA]”, but does not stipulate that organisations may not designate individuals already designated by other organisations. Section 11(4) of the PDPA further provides that an individual designated by an organisation may further delegate the responsibility to another individual. For the avoidance of doubt, the designated individual need not be an employee of the organisation.

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

There are no specific qualifications required by law of the DPO. In practice, however, it is advisable that an organisation appoint an individual (or a group of individuals) familiar with the data protection laws of Singapore, the organisation's data protection policies and procedures, as well as its data processing activities. This is to ensure that the DPO is well equipped to: (i) ensure the organisation's continued compliance with the PDPA; (ii) deal with any queries from authorities or the public in relation to the organisation's data protection practices; and (iii) limit the impact of any data breach incident.

The PDPC has also published the DPO Competency Framework and Training Roadmap to provide clarity on the competencies and proficiency levels that a DPO needs, and to assist organisations in the hiring and training of data protection professionals.

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

The DPO is responsible for ensuring the organisation's continued compliance with the PDPA. However, it should be noted that the appointment of a DPO does not relieve the organisation of its obligations and liabilities under the PDPA.

Some of the responsibilities of a DPO may include, but are not limited to:

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

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

No, there is no requirement for the DPO to be registered with or notified to the PDPC. However, DPOs are encouraged to register themselves with the PDPC to gain access

to free workshops and resources, latest updates on the PDPA and best practices, exclusive networking events and insights on key trends for data breach prevention. DPOs may register themselves with the PDPC via its website, where they may keep abreast of developments in the PDPA and best practices: <https://www.pdpc.gov.sg/overview-of-pdpa/data-protection/business-owner/data-protection-officers>

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

No. However, under the PDPA, the business contact information of at least one DPO must be made available to the public. Under the PDP Regulations, this requirement is deemed to have been satisfied if the organisation makes available such information in any of the following manners:

- where the organisation is registered under an applicable Act – in a record relating to the organisation that is made available on the Internet website of the Accounting and Corporate Regulatory Authority at <https://www.bizfile.gov.sg> (at the time of writing, this website is unavailable); or
- in a readily accessible part of the organisation's official website.

9 Appointment of Processors

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

The PDPA does not expressly stipulate that an organisation must enter into an agreement with its data intermediary. However, it should be noted that appointing a data intermediary to process personal data does not relieve the organisation of its obligations and liabilities under the PDPA, as the organisation is deemed to “have the same obligation under [the PDPA] in respect of personal data processed on its behalf and for its purposes by a data intermediary as if the personal data were processed by the organisation itself”. In this regard, the PDPC's Guide to Managing Data Intermediaries states that the primary means by which an organisation may ensure appropriate protection of the personal data processed by its data intermediary is through a contract, and that it would be a breach of the PDPA if there is no contractual agreement or document setting out the key obligations and responsibilities of the data intermediary.

Further, the Advisory Guidelines on Key Concepts in the Personal Data Protection Act (“**Key Concepts Guidelines**”) state that it is important that an organisation is clear as to its rights and obligations when dealing with another organisation and, where appropriate, include provisions in their written contracts to clearly set out each organisation's responsibilities and liabilities in relation to the personal data in question, including whether one organisation is to process personal data on behalf of and for the purposes of the other organisation. Without clarity, the risks of any omissions will likely fall on the organisation, which as data controller, is ultimately responsible. If there is no contract evidenced or made in writing with the data organisation, the data intermediary may also be held directly responsible for the Data Protection Provisions in respect of the personal data that is processed on behalf of the data organisation.

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

As the organisation remains responsible for complying with the PDPA, notwithstanding that a data intermediary is processing personal data on its behalf, the organisation should set out clearly the responsibilities of all parties and impose specific obligations on its data intermediary through a written agreement, including restricting what the data intermediary may do with the disclosed personal data, having sufficient security measures to protect the disclosed personal data, and providing for audits, inspections or other types of spot checks to satisfy itself that the data intermediary is complying with the PDPA as well as exit management. The contractual terms should also reference a relevant international standard as the standard for protection of the personal data. In setting out the contract, the organisation should also consider and review details such as the schedules to the contract and other administrative instructions outside the contract. These can be developed in consultation with the data intermediary.

If it is contemplated that there will be overseas transferees of personal data, the agreement should provide assurances to ensure that the transferred personal data will remain protected to a standard comparable with the PDPA, along with other policies and practices (e.g. assurances of compliance with relevant industry standards/certification). See the “Transfer Limitation Obligation” at section 12 below.

10 Marketing

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

The PDPA and the SCA concurrently govern the sending of such direct marketing messages in Singapore.

Generally, where the personal data of an individual is collected, used and disclosed for marketing purposes, the consent of the individual concerned must be obtained and such consent must not have been obtained as a condition for the providing of a product or service where it would not be reasonably required to provide that product or service. This applies regardless of how the marketing communications are sent.

In this regard, the PDPC has noted in its Key Concepts Guidelines that a failure to opt out will not be regarded as consent in all situations, and has recommended that organisations obtain consent from an individual through a positive action of the individual. It would therefore be advisable to obtain prior opt-in consent instead.

In relation to the sending of marketing communications (i.e. “specified messages” as defined under Section 37 of the PDPA) by telephone call or text messaging (or fax) to a Singapore telephone number, the DNC Provisions of the PDPA require an organisation to:

- (a) obtain valid confirmation that the telephone number is not listed with the relevant DNC Register before sending the message or calling, unless clear and unambiguous consent to the sending of the specified message to that number is obtained in evidential form;
- (b) include information identifying the sender for messages and details on how the sender can be readily contacted

and such details and contact information should be reasonably likely to be valid for at least 30 days after the sending of the message;

- (c) for voice calls, not conceal or withhold the calling line identity from the recipient; and
- (d) not to send, cause to be sent, or authorise the sending of an applicable message to any telephone number generated or obtained through the use of: (i) a dictionary attack; or (ii) address-harvesting software.

In relation to the sending of unsolicited marketing communications in bulk by email, instant messaging or other electronic messaging means, Section 11 read with the Second Schedule of the SCA stipulates that such messages must contain, *inter alia*, the following:

- (a) information on the sender;
- (b) a clear and conspicuous statement in English setting out the procedure to unsubscribe;
- (c) a title in its subject field that is not false or misleading as to the content of the message;
- (d) a label “<ADV>” with a space before the title of the subject field or, in the absence of a subject field, the first word of the message;
- (e) header information that is not false or misleading; and
- (f) an accurate and functional email address or telephone number by which the sender is readily contactable.

The unsubscribe facility must be legitimately obtained, valid and capable of receiving the unsubscribe request and a reasonable number of similar unsubscribe requests sent by other recipients at all times within at least 30 days after the unsolicited message is sent. No further unsolicited marketing communications can be sent after 10 business days following the date of the unsubscribe request.

Furthermore, Section 9 of the SCA prohibits unsolicited commercial electronic messages in bulk from being sent to electronic addresses generated or obtained through the use of a dictionary attack or address-harvesting software.

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

Generally, the direct marketing restrictions in the PDPA only apply in the business-to-consumer (“B2C”) context where an organisation sends direct marketing communications to individual consumers. Insofar as an organisation sends direct marketing messages to another organisation through the use of business contact information, i.e. business-to-business (“B2B”) messages, the PDPA would likely not be applicable in those instances.

Specifically in relation to the sending of specified messages (as defined in Section 37 of the PDPA) by telephone call, text messaging, or fax to a Singapore telephone number, paragraph 1(g) of the Eighth Schedule of the PDPA provides that a “specified message” shall exclude “any message sent to an organisation other than an individual acting in a personal or domestic capacity, for any purpose of the receiving organisation”. In other words, a B2B marketing message would not be considered a “specified message”, and the organisation that sent such a B2B message would not need to comply with requirements under the DNC Provisions.

Notwithstanding, B2B marketing is currently covered under the SCA, and the restrictions on such electronic messages (see question 10.1 above) would similarly apply.

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

Please see our response to question 10.1 above.

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

Yes, insofar as an organisation collects, uses or discloses personal data in Singapore (e.g. collects the personal data from individuals in Singapore for marketing purposes), the Data Protection Provisions of the PDPA would apply to such organisation, whether or not the organisation is formed or recognised under the laws of Singapore, or resident or having an office or a place of business in Singapore.

Specifically, the DNC Provisions under the PDPA apply when the sender of the specified message is present in Singapore when the specified message is sent, or the recipient of the specified message is present in Singapore when the specified message is accessed.

The SCA applies as long as the electronic message has a Singapore link, which includes, *inter alia*, the following situations:

- the message originates in Singapore or the sender of the message is: (i) an individual who is physically present in Singapore when the message is sent; or (ii) an entity which is formed or recognised under the law of Singapore, or which has an office or a place of business in Singapore;
- the computer, mobile telephone, server or device that is used to access the message is located in Singapore; or
- the recipient of the message is, when the message is accessed: (i) an individual who is physically present in Singapore; or (ii) an entity that carries on business or activities in Singapore.

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

The PDPA is a complaints-based regime and the PDPC has been active in the enforcement of breaches thereof.

Since the commencement of the PDPA in 2014, the PDPC has charged several individuals for offences relating to breaches of the DNC Registry.

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

Purchasing marketing lists from third parties is only lawful if the individuals whose personal data is contained within the lists are notified of, and consent to, the sale of their personal data before such data is collected, used and/or disclosed.

The purchase of marketing lists constitutes collecting personal data under the PDPA. The PDPC has taken enforcement action against organisations which have purchased marketing lists without obtaining valid consent. For example, in the decision of *Re Sharon Assya Qadriyah Tang* [2018] SGPDP 1, the PDPC imposed a financial penalty of S\$6,000 on an individual for buying and selling marketing lists containing personal data.

Similarly, the PDPC took action in the case of *Re Amicus Solutions Pte Ltd & Anor* [2019] SGPDP 33, which involved the unauthorised sale and disclosure of personal data by a data broker for telemarketing purposes. In that case, the PDPC stated that organisations that sell datasets should ensure that they obtain and maintain clear records of consent so that proper assurances can be given to buyers. Correspondingly, buyers should undertake proper due diligence, such as seeking written confirmation that the personal data sold was actually obtained via legal sources or means, or inquire further as to whether the individuals were notified of the disclosure and had provided consent, and if so, obtain a sample of such notification and consent. On the facts, the PDPC imposed a fine of S\$48,000 on the data seller (including the S\$2,900 for the profit that the seller made from the sale of the datasets), and a fine of S\$10,000 on the buyer.

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

In relation to a breach of the Data Protection Provisions that apply to the sending of marketing communications, the organisation may find itself liable to pay a financial penalty of up to S\$1 million or 10% of the organisation's annual turnover in Singapore, whichever is higher. See question 8.2 above.

In relation to the DNC Provisions, the Amendment Act brings contraventions of the DNC Provisions (which used to be enforced as criminal offences), under the same administrative regime as the Data Protection Provisions. Accordingly, if the organisation is found to have intentionally or negligently contravened any provision, the PDPC may require the organisation to pay a financial penalty not exceeding:

- (a) S\$200,000, in case of an individual; or
- (b) S\$1 million, in any other case.

For contravention of the provisions prohibiting the use of dictionary attacks and address-harvesting software under the DNC Provisions, the maximum financial penalty has been increased to 5% of the annual turnover of the organisation in Singapore, where the annual turnover in Singapore exceeds S\$20 million.

These offences are in addition to the rights of private action that individuals may have against the organisation under the PDPA and the SCA.

11 Cookies

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

There are presently no legislative restrictions on the use of cookies or similar technologies *per se*, although the PDPA will apply to cookies that collect or use personal data.

According to the Advisory Guidelines on the PDPA for Selected Topics, for Internet activities that the user has clearly requested (e.g. transmitting personal data for effecting online communications and storing information that the user enters in a web form to facilitate an online purchase), there may not be a need to seek consent for the use of cookies to collect, use and disclose personal data where the individual is aware of the purposes for such collection, use or disclosure and voluntarily provided his personal data for such purposes. For activities that cannot take place without cookies that collect, use or disclose personal data, consent may be deemed if the

individual voluntarily provides the personal data for that purpose of the activity, and it is reasonable that he would do so. The Guidelines also clarify that the mere failure of an individual to actively manage his browser settings does not imply that the individual has consented to the collection, use and disclosure of his personal data by all websites for their stated purpose.

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

This is not applicable in Singapore.

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

This is not applicable in Singapore.

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

This is not applicable in Singapore.

12 Restrictions on International Data Transfers

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

The Transfer Limitation Obligation under the PDPA requires organisations transferring personal data overseas to do so only in accordance with the requirements prescribed under the PDPA to ensure that the recipients provide the transferred personal data a standard of protection that is comparable to the PDPA.

In particular, under the PDP Regulations, the transferring organisation must, before transferring the personal data outside of Singapore, take appropriate steps to ascertain whether, and to ensure that, the recipient is bound by legally enforceable obligations to provide the transferred personal data with a standard of protection comparable to that under the PDPA.

Pursuant to Regulation 11(1) of the PDP Regulations, “legally enforceable obligations” include obligations imposed on the recipient under:

- (a) any law;
- (b) any contract that requires the recipient to provide to the transferred personal data a standard of protection that is at least comparable to the protection under the PDPA, and which specifies the countries and territories to which the personal data may be transferred under the contract;
- (c) any binding corporate rules (in cases where a recipient is an organisation related to the transferring organisation) that require every recipient to provide to the transferred personal data a standard of protection that is at least comparable to the protection under the PDPA, and which specifies (i) the recipients of the transferred personal data to which the binding corporate rules apply, (ii) the countries and territories to which the personal data may be transferred under the binding corporate rules, and

(iii) the rights and obligations provided by the binding corporate rules; or

(d) any other legally binding instrument.

In relation to binding corporate rules, the PDP Regulations define a recipient as being related to the transferring organisation if:

- (a) the recipient, directly or indirectly, controls the transferring organisation;
- (b) the recipient is, directly or indirectly, controlled by the transferring organisation; or
- (c) the recipient and the transferring organisation are, directly or indirectly, under the control of a common person.

For completeness, the PDP Regulations provide for certain prescribed situations whereby the Transfer Limitation Obligation is taken to be satisfied and it is not necessary to legally impose enforcement obligations, e.g. where the personal data is publicly available in Singapore or where the personal data is data in transit.

The PDP Regulations also recognise the certification systems under the Asia-Pacific Economic Cooperation (“APEC”) Cross-Border Privacy Rules (“CBPR”) System and Privacy Recognition for Processors (“PRP”) System as one of the modes for the transfers of data overseas. If the recipient holds a specified certification (i.e. certification under the APEC CBPR/PRP) that is granted or recognised under the law of that country or territory to which the personal data is transferred, the recipient is taken to be bound by legally enforceable obligations to provide a standard of protection for the transferred personal data that is at least comparable to the protection under the PDPA.

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

Companies generally rely on robust data transfer agreements and binding corporate rules, as well as active enforcement of the terms of these documents, to ensure their compliance with applicable transfer restrictions.

See also questions 9.1 and 9.2 above with respect to overseas transfers of personal data for organisations engaging data intermediaries.

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

No, there is no requirement for registration/notification or prior approval from the PDPC for transfers of personal data abroad.

12.4 Do transfers of personal data to other jurisdictions require a transfer impact assessment? If conducting a transfer impact assessment is only mandatory in some circumstances, please identify those circumstances.

The PDPA does not require organisations to carry out a

transfer impact assessment (which is not a term defined under the PDPA) when transferring personal data outside of Singapore. There is no express requirement to assess whether the laws and practices in the third country prevent the overseas recipient from providing the requisite standard of protection, in particular, taking into account the rights of access and surveillance by the third country's public authorities.

However, for clarity, one of the available transfer mechanisms under the PDPA is for the transferring organisation to assess and determine that the foreign national laws governing the overseas recipient of the transferred personal data provides a standard of protection comparable to that under the PDPA (i.e. this is a way of ensuring that there are legally enforceable obligations imposed on the recipient, pursuant to Regulation 11(1)(a) of the PDP Regulations).

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

The PDPC has not issued any guidance on this topic.

12.6 What guidance (if any) has/have the data protection authority(ies) issued in relation to the use of standard contractual/model clauses as a mechanism for international data transfers?

The PDPC, in collaboration with ASEAN and the EU, has published a Joint Guide to ASEAN Model Contractual Clauses (“ASEAN MCCs”) and EU Standard Contractual Clauses (“EU SCCs”), which was updated on 31 January 2024. The non-binding guide, which comprises a Reference Guide and an Implementation Guide, provides organisations looking to transfer or receive data from overseas partners with a comparison between the ASEAN MCCs and EU SCCs and examples of best practices that can be implemented to operationalise safeguards required under the ASEAN MCCs and EU SCCs.

13 Whistle-blower Hotlines

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

The PDPA does not specifically regulate corporate whistle-blowing hotlines.

To the extent that whistle-blowing falls under the definition of “investigation” as found in the PDPA, the PDPA provides that personal data can be collected without obtaining consent if it is necessary for any investigation or proceedings. Similarly, the use and disclosure of personal data can be done without obtaining consent if it is necessary for any investigation or proceedings.

In this regard, the PDPA defines “investigation” to refer to an investigation relating to:

- (a) a breach of an agreement;
- (b) a contravention of any written law, or any rule of professional conduct or other requirement imposed by any regulatory authority in exercise of its powers under any written law; or

- (c) a circumstance or conduct that may result in a remedy or relief being available under any law.

The PDPA also provides for a broad definition of “proceedings” to mean any civil, criminal or administrative proceedings by or before a court, tribunal or regulatory authority that is related to the allegation of:

- (a) a breach of an agreement;
- (b) a contravention of any written law or any rule of professional conduct or other requirement imposed by any regulatory authority in exercise of its powers under any written law; or
- (c) a wrong or a breach of a duty for which a remedy is claimed under any law.

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

Anonymous reporting is not regulated under the PDPA.

14 CCTV

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

The PDPA does not require the use of CCTV to be separately registered/notified or approved beforehand by the PDPC. However, as video and audio recordings of individuals may constitute personal data, the use of CCTV may constitute the collection of personal data and hence an organisation must comply with the PDPA when using CCTV.

According to the PDPC's Advisory Guidelines on the PDPA for Selected Topics, the PDPC recommends that notices or other forms of notification should generally be placed at locations that would enable individuals to have sufficient awareness that CCTV has been deployed for a particular purpose. Generally, organisations should indicate that CCTV is operating in the premises, and state the purpose of the CCTV (e.g. the CCTV is installed for security purposes) if such purpose may not be obvious to the individual. Further, where the CCTV deployed records both video and audio, organisations should indicate that both video and audio recordings are taking place.

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

Insofar as CCTV data contains personal data, the PDPA limits the purposes for which the CCTV data may be used.

15 Employee Monitoring

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

Employee monitoring is not specifically regulated in Singapore. To the extent that the employee monitoring results in the collection, use or disclosure of personal data under the PDPA, such monitoring must comply with the Data Protection Provisions.

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

Employers are generally required to provide suitable notices and obtain consent, before collecting, using or disclosing the personal data of their employees.

However, the PDPA provides for an exception to consent where personal data is collected by the employer and the collection for the purpose of or in relation to the organisation: (a) entering into an employment relationship with the individual or appointing the individual to any office; or (b) managing or terminating the employment relationship with or appointment of the individual. Nonetheless, if the organisation wishes to rely on this exception, the organisation would need to inform the individual of the purpose, and on request by the individual, the contact information of a person who is able to answer the individual's questions on such processing.

The "legitimate interests" exception to consent may also be applicable. However, the organisation would similarly need to notify the individual that it is relying on the exception for such purposes (and comply with other conditions).

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

As the relationship between employers and trade unions is very much subject to the terms of the collective agreement, the necessity of notifying or consulting the trade union in respect of CCTV and employee monitoring is dependent on the terms of the collective agreement. There are generally no legal requirements under Singapore law requiring works councils/trade unions/employee representatives to be notified or consulted.

15.4 Are employers entitled to process information on an employee's attendance in office (e.g., to monitor compliance with any internal return-to-office policies)?

Employers can process information on an employee's attendance in office for reasons such as monitoring compliance with internal return-to-office policies without the employee's consent if this is reasonable for managing the employment relationship. However, the employers must first notify their employees of the purposes of processing of personal data. Please see our response to question 15.2 above for more information on this exception.

16 Data Security and Data Breach

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

Yes, both organisations and data intermediaries are subject to the Protection Obligation in relation to the personal data in their possession or control. For the Protection Obligation, please see our response to question 4.1 above.

While the PDPC has recognised that there is no one-size-fits-all solution, it has, in its Key Concepts Guidelines, noted that an organisation should:

- design and organise its security arrangements to fit the nature of the personal data held by the organisation

and the possible harm that might result from a security breach;

- identify reliable and well-trained personnel responsible for ensuring information security;
- implement robust policies and procedures for ensuring appropriate levels of security for personal data of varying levels of sensitivity; and
- be prepared and able to respond to information security breaches promptly and effectively.

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

There is a mandatory data breach notification regime under Part 6A of the PDPA, which broadly requires organisations to notify the PDPC of a "notifiable data breach".

Duty to assess

Section 26C of the PDPA requires organisations to conduct, in a reasonable and expeditious manner, an assessment of whether the data breach is a notifiable data breach, if it has reason to believe that a data breach has occurred affecting personal data in its possession or under its control.

Where a data intermediary has reason to believe that a data breach has occurred in relation to personal data that the data intermediary is processing on behalf of and for the purposes of another organisation, the data intermediary must, without undue delay, notify that other organisation of the occurrence of the data breach.

Requirement to notify

Under Section 26D of the PDPA, a data breach is a "notifiable data breach" if it:

- results in, or is likely to result in, significant harm to the individuals to whom the data relates (including if the breach relates to prescribed types of data); or
- is, or is likely to be, of a significant scale (i.e. the data breach involves personal data of 500 or more individuals).

The organisation must notify the PDPC as soon as is practicable, but in any case, no later than three calendar days after it makes the assessment.

The notification should be in the form and manner as prescribed in the Personal Data Protection (Notification of Data Breaches) Regulations 2021 and contain information to the best of the knowledge and belief of the organisation at the time.

Details of notification

Specifically, the notification to the PDPC should include information such as:

- the date and circumstances in which the organisation first became aware that the data breach had occurred;
- an account of steps taken afterwards, including the organisation's assessment of whether the breach is notifiable;
- how the data breach occurred;
- the number of individuals affected by the data breach;
- the personal data or classes of personal data affected;
- the potential harm to the affected individuals as a result;

- any action by the organisation to: (i) eliminate or mitigate any potential harm to any affected individual; and (ii) address or remedy any failure or shortcoming that resulted in the breach;
- the organisation's plan to inform all or any affected individuals or the public or grounds for not informing the affected individuals (if applicable);
- the business contact information of at least one authorised representative; and
- the reasons for late notification and/or the grounds for not notifying affected individuals (if the organisation is otherwise required to notify), where applicable.

Notification to the PDPC is to be submitted at <https://eservice.pdpc.gov.sg/case/db> For urgent notification of major cases, organisations may also contact the PDPC at +65 6377 3131 during working hours.

The PDPC's Guide on Managing and Notifying Data Breaches (updated 15 March 2021) provides further guidance to help organisations to identify, prepare for and manage data breaches.

In addition to the Data Breach Notification Obligation under the PDPA, there may also be sector-specific requirements relating to the notification of data breaches to which the organisation is subject.

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

Under Section 26D of the PDPA, organisations must, on or after notifying the PDPC, notify the individuals affected by a notifiable data breach, if the data breach results in, or is likely to result in, significant harm to an affected individual, unless either one of the stated exceptions apply, namely:

- where the organisation has taken remedial action that renders it unlikely that the notifiable data breach will result in significant harm to the affected individual;
- where the organisation has implemented any technological measure (e.g. encryption) that renders it unlikely that the notifiable data breach will result in significant harm to the affected individual; or
- if the organisation is instructed by a prescribed law enforcement agency, or directed by the PDPC, not to notify any affected individual.

In addition, the PDPC may, on written application, waive the requirement in exceptional circumstances where notification to affected individuals may not be desirable.

The notification to affected individuals should contain the following:

- the circumstances in which the organisation first became aware that the data breach had occurred;
- the personal data or classes of personal data affected;
- the potential harm to the affected individuals as a result;
- any action by the organisation to: (i) eliminate or mitigate any potential harm to any affected individual; and (ii) address or remedy any failure or shortcoming that resulted in the breach;
- the steps that the affected individual may take to eliminate or mitigate any potential harm as a result, including preventing the misuse of the data; and
- contact details of at least one authorised representative whom the affected individual can contact for further information or assistance.

The notification should be in the form and manner as prescribed in the Personal Data Protection (Notification of Data Breaches) Regulations 2021 and contain information to the best of the knowledge and belief of the organisation at the time.

16.4 What are the maximum penalties for personal data security breaches?

The PDPC has discretion to issue such remedial directions as it sees fit, including a notice to require payment of a financial penalty of up to a maximum of 10% of the organisation's annual turnover in Singapore, or S\$1 million, whichever is higher.

On 15 January 2019, the PDPC imposed its highest financial penalties to date, of S\$250,000 and S\$750,000, respectively, on SingHealth Services Pte Ltd ("SingHealth") and Integrated Health Information Systems Pte Ltd, for breaching their data protection obligations under the PDPA. This unprecedented data breach, which arose from a cyberattack on SingHealth's patient database system, caused the personal data of some 1.5 million patients to be compromised.

17 Enforcement and Sanctions

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

- (a) **Investigative powers:** The Ninth Schedule of the PDPA sets out extensive powers of investigation of the PDPC and its inspectors, which includes the power to: (i) require documents or information; (ii) require provision of information (e.g. to require attendance of individuals); and (iii) enter premises with or without a court-issued search warrant.

Section 51 of the PDPA sets out certain offences relating to, amongst others, obstructing or hindering the PDPC in the performance of any function or duty, or the exercise of any power, under the PDPA. It is also an offence for an organisation or a person, without reasonable excuse, to neglect or refuse to either provide any information or produce any document which the organisation or person is required to provide or produce to the PDPC or an inspector, or attend before the PDPC or inspector as required.

- (b) **Corrective powers:** Under Section 48H of the PDPA, upon a complainant's application, the PDPC may review: (i) refusals to provide access to personal data or to correct personal data as requested by the complainant under the PDPA or a failure to provide such access or correction within a reasonable time; and (ii) a fee required from the complainant by an organisation in relation to a request by the complainant under the PDPA.

Upon reviewing, the PDPC may: (i) confirm the refusal to provide access to or correct the personal data (as the case may be) or direct the organisation to provide access to or correct the personal data (as the case may be) within a specified timeframe; or (ii) confirm, reduce or disallow a fee, or direct the organisation to make a refund to the complainant.

- (c) **Authorisation and advisory powers:**

- Voluntary undertakings

Section 48L of the PDPA empowers the PDPC to accept statutory undertakings. Under this new

Section, where the PDPC has reasonable grounds to believe that an organisation has not complied, is not complying or is likely not to comply with any of the Data Protection Provisions, the organisation may give, and the PDPC may accept a written voluntary undertaking.

■ **Alternative dispute resolution**

Section 48G of the PDPA empowers the PDPC to establish or approve one or more dispute resolution schemes for the resolution of complaints by mediation, and to make regulations relating to the operation of such schemes. The PDPC may, with or without the parties' consent, refer the matter to mediation under a dispute resolution scheme, if it is of the view that the matter may more appropriately be resolved in this manner.

The PDPC has issued a Guide on Active Enforcement which articulates the PDPC's approach in deploying its enforcement powers to act effectively and efficiently in the event of data breach incidents. The guide also reiterates the PDPC's general approach to maximise the use of facilitation and mediation in seeking a resolution between the complainant and the organisation concerned.

- (d) **Imposition of administrative fines for infringements of specified legal provisions:** In the context of Singapore, the PDPC may impose a financial penalty of up to a maximum of 10% of the organisation's annual turnover in Singapore, or S\$1 million, whichever is higher, for breaches of the Data Protection Provisions in the PDPA.

In the event of a breach of the DNC Provisions of the PDPA, the PDPC may require the organisation to pay a financial penalty not exceeding:

- (a) S\$200,000, in case of an individual; or
(b) S\$1 million, in any other case,

except that for contravention of the provisions prohibiting the use of dictionary attacks and address-harvesting software under the DNC Provisions, the maximum financial penalty has been increased to 5% of the annual turnover of the organisation in Singapore, where the annual turnover in Singapore exceeds S\$20 million.

- (e) **Non-compliance with a data protection authority:** If the PDPC is satisfied that: (a) an organisation has not complied or is not complying with any provision of the Data Protection Provisions; or (b) a person has not complied or is not complying with any of the DNC Provisions, the PDPC may issue such directions as it thinks fit in the circumstances to ensure compliance by an organisation with the PDPA. These include, but are not limited to, directions to: (i) stop collecting, using or disclosing personal data in contravention of the PDPA; (ii) destroy personal data collected in contravention of the PDPA; (iii) comply with any direction of the PDPC; and (iv) pay a financial penalty. (Please see question 17.1(d) above on the quantum of the financial penalty.)

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

The PDPC is empowered to direct an organisation to stop collecting, using or disclosing personal data in contravention of the PDPA.

The PDPC does not require a court order to issue directions. Nonetheless, the PDPC may apply for the direction to be registered in a District Court for the purposes of enforcement by the court.

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

The PDPC takes a pragmatic approach in administering and enforcing the PDPA and aims to balance the need to protect individuals' personal data and the needs of organisations to use the data for legitimate purposes.

Since 2016, the PDPC has published over 250 enforcement decisions, with a significant majority of these cases relating to breaches of the Protection Obligation. In respect of these cases, the PDPC has either issued the organisation a warning, or imposed directions requiring the infringing organisation to take remedial action and to pay financial penalties.

Examples of recent cases include the following:

- A financial penalty of S\$20,000 was imposed on the Consumers' Association of Singapore (a non-profit, non-governmental organisation which aims to protect consumer interests) for its breach of the Protection and Accountability Obligations in respect of two data breach incidents. The first incident involved a threat actor signing into the organisation's email accounts using login credentials that were likely obtained from a successful phishing attack on an employee. The threat actor was thereby able to harvest consumers' email addresses from the organisation's mailboxes and send phishing emails on behalf of the organisation with the organisation's verified domain name. Three individuals suffered monetary losses. The second incident relates to the sending of phishing emails to consumers (which contained the details of their original complaints to the organisation) but not from the organisation's domain. The exfiltration of such data likely arose when the organisation migrated data from one vendor to another. With regard to the Protection Obligation, the PDPC found that the organisation's password management policy was manifestly insufficient. It failed to enforce the minimum character-length stated in its Password Complexity Policy, and did not adopt/enforce how frequently passwords ought to be changed. The organisation also failed to stipulate clear security responsibilities in its vendor contracts and conduct staff training. With regard to the Accountability Obligation, the Organisation failed to have any ICT policies to cover critical aspects in its IT security, among other things. In determining the financial penalty, the Commission also considered the organisation's turnover.
- A financial penalty of S\$120,000 was imposed on Keppel Telecommunications & Transportation for a breach of the Protection Obligation under the PDPC. The PDPC found that the organisation had failed to implement reasonable security arrangements to protect the personal data of employees, ex-employees, directors and shareholders in its possession or under its control. Notably, the PDPC observed that the long period of the organisation's breach of the Protection Obligation (i.e. more than two years), and the organisation's failure to provide clear instructions and supervise staff during its data migration and divestment (in particular, to delete its personal data from the affected server belonging to

the divested entity) revealed systemic shortcomings in the organisation's data protection processes. The PDPC also noted that the affected data included specimen signatures, bank account numbers, full images of identification cards, among others, which exposed individuals to greater risks of identity theft or financial losses. In determining the financial penalty, the Commission also considered the organisation's turnover to ensure the penalty would be an effective deterrent.

- A financial penalty of S\$7,000 was imposed on Tok Leng Leng t/a Top Mobile Gallery (BR) for breaching the Protection Obligation under the PDPA. The organisation had failed to implement reasonable security arrangements to protect against the unauthorised use of and access to customers' personal data for registration of pre-paid SIM cards. Specifically, the organisation did not maintain an inventory of SIM cards, failed to account for individuals to whom the SIM cards were registered, and allowed multiple employees to share login credentials on personal devices. The organisation had also exercised little or no supervision over their employees regarding how they used or accessed the customer's personal data.
- A financial penalty of S\$28,000 was imposed on Horizon Fast Ferry for failing to put in place reasonable security arrangements to protect its platform users' personal data in its possession or under its control. The organisation did not have its own IT department and relied informally on the goodwill of an employee of its overseas IT vendor to provide support. The organisation was found to have lacked basic IT security measures, including an ICT policy, vendor management protocols and security controls for its web server. It had no formal agreement with its IT vendor and failed to ensure that root account credentials were properly managed or deactivated after termination of service contracts. This resulted in the unauthorised access and exfiltration of users' personal data. The PDPC also noted this was not the organisation's first instance of non-compliance with the PDPA.
- A financial penalty of S\$74,000 was imposed on PPLingo for breaches of the Protection and Accountability Obligations. At the time of the incident, the organisation had in place a data protection policy and had implemented certain security measures for its platform, including network access control measures and firewall protection. The organisation also organised two rounds of awareness training for its IT development team one month before the incident. Nevertheless, given the high volume and sensitivity of the data, the onus was on the organisation to implement an appropriately robust level of security arrangements to satisfy the Protection Obligation. The PDPC found that the organisation had failed to put in place reasonable security arrangements to protect the personal data of over 557,000 users, including minors and individuals whose data included sensitive financial information. This included its failure to implement adequate password policies, such as mandating a minimum level of password complexity. The PDPC also noted that PPLingo had failed to appoint a Data Protection Officer since its incorporation in 2016, contrary to its obligations under the PDPA.

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

We have not sighted a published decision whereby the PDPC

has exercised its powers against companies established in other jurisdictions with no presence in or nexus to Singapore. That said, the PDPC investigated a company established overseas which collected the personal data of Singapore residents through a registered branch office (see, e.g. *Re Cigna Europe Insurance Company S.A.-N.V.* [2019] SGPDP18).

Nonetheless, the PDPC is empowered to enter into a cooperation agreement with a foreign data protection authority for data protection matters such as cross-border cooperation. Specifically, under Section 10 of the PDPA, cooperation agreements may be entered into for the purposes of:

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

The PDPC may also furnish information to a foreign data protection body pursuant to a cooperation agreement, subject to the fulfilment of certain prescribed conditions.

The PDPC is also a participant of the APEC Cross-Border Privacy Enforcement Arrangement, which creates a framework for the voluntary sharing of information and provision of assistance for privacy enforcement-related activities.

18 E-discovery/Disclosure to Foreign Law Enforcement Agencies

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

Generally, organisations must ensure that any transfers of personal data outside of Singapore comply with the requirements under the PDPA (see our responses in section 12 above). It is not uncommon for Singapore businesses to include, in their privacy policy, a general notice that any personal data they collect may be disclosed to foreign law enforcement agencies or in relation to investigations and legal proceedings.

18.2 What guidance has/have the data protection authority(ies) issued on disclosure of personal data to foreign law enforcement or governmental bodies?

The PDPC has not issued any specific guidance yet in relation to the disclosure of personal data to foreign law enforcement or governmental bodies.

19 Artificial Intelligence

19.1 Are there any limitations on automated decision-making involving the processing of personal data using artificial intelligence?

The PDPA does not impose any specific limitations to automated decision-making that processes personal data in AI systems. However, where the automated decision-making system involves the collection, use or disclosure of personal data, the general Data Protection Provisions would apply.

19.2 What guidance (if any) has/have the data protection authority(ies) issued in relation to the processing of personal data in connection with artificial intelligence?

In its Advisory Guidelines on the Use of Personal Data in AI Recommendation and Decision Systems (issued on 1 March 2024), the PDPC highlighted that when organisations deploy AI systems in their services or products that collect, use or disclose personal data to provide new functionalities or to conduct automated decision-making, they should be mindful of the Consent (Sections 13 to 20 of the PDPA), Notification (Section 20 of the PDPA), and Accountability (Sections 11 and 12 of the PDPA) Obligations.

In particular, the Consent and Notification obligations under the PDPA operate in tandem to ensure that individuals are informed and their participation is meaningful. When organisations rely on AI systems to process personal data for decision-making purposes, they must inform individuals of the purposes of collection and intended uses of their data at the point of obtaining consent. This ensures that any consent provided is informed and meaningful.

The PDPC recommends that organisations provide, to the extent practicable:

- a clear explanation of the functionality of the product or service that relies on personal data;
- a general description of the types of data being collected and processed;
- details of how the data processing supports the product feature; and
- the specific data attributes that are likely to influence the AI output or decision.

Where organisations assess that it is necessary to limit the detail provided in favour of a more general explanation due to commercial sensitivity or security concerns over its AI systems, they are expected to document their justifications internally.

Furthermore, under the Accountability Obligation, organisations must be transparent in their use of AI systems. This includes maintaining internal policies and safeguards that promote fairness and reasonableness in how decisions are made. The depth of transparency expected is proportionate to the risks involved in each use case, such as the potential harm to individuals or the extent to which the AI system operates autonomously.

20 Trends and Developments

20.1 In your opinion, what enforcement trends have emerged during the previous 12 months? Describe any relevant case law or recent enforcement actions.

Breaches of the Protection Obligation under the PDPA continue to constitute the majority of enforcement decisions issued by the PDPC, with the majority of cases over the past 12 months involving the Protection Obligation.

20.2 In your opinion, what “hot topics” are currently a focus for the data protection regulator?

New PDPC Guides Concerning Children’s Personal Data and AI

On 28 March 2024, the PDPC published the Children’s Personal Data Guidelines. Please see our response to question 6.1 for more information.

On 1 March 2024, the PDPC published its Advisory Guidelines on Use of Personal Data in AI Recommendation and Decision Systems. The guidelines provide guidance on how the PDPA applies when organisations use personal data to develop and train AI systems and set out best practices for how service providers (e.g. systems integrators) may support organisations implementing bespoke or fully customisable AI systems.

New and Updated ASEAN Guides

On 2 February 2024, during the 4th ASEAN Digital Ministers’ Meeting, the ASEAN Guide on AI Governance and Ethics (“**ASEAN AI Guide**”) and the updated Joint Guide to ASEAN MCCs and EU SCCs were launched. The ASEAN AI Guide sets out common principles for trustworthy AI and best practices for implementation in ASEAN. Please see our response to question 12.6 regarding the updated Joint Guide to ASEAN MCCs and EU SCCs.

At the 5th ASEAN Digital Ministers’ Meeting held in Bangkok, Thailand, on 16 to 17 January 2025, several initiatives were introduced to enhance the regulation and facilitation of cross-border data flows:

- A Joint Guide comparing the ASEAN MCCs with the Ibero-American Data Protection Network (“**RIPD**”) MCCs was published. It aims to help businesses, particularly companies already familiar with the ASEAN MCCs, to navigate contractual negotiations for international data transfers with their RIPD business partners.
- The ASEAN–China 2025 Digital Work Plan was endorsed, featuring a Joint Guide that maps ASEAN MCCs against China’s Standard Contractual Clauses for cross-border data flows. While not legally binding, these guides are expected to aid multinational businesses in understanding the interplay between various regional frameworks, thereby easing compliance.
- The meeting acknowledged the efforts of the ASEAN Working Group on Digital Data Governance in advancing the use and interoperability of ASEAN MCCs, including its collaboration with the Ibero-American Data Protection Network. It also welcomed the Operational Framework for Global CBPR and PRP, and encouraged ASEAN Member States to adopt these certification systems to promote trust, support cross-border data movement and bolster the regional digital economy.



Lim Chong Kin is the Managing Director of Drew & Napier's Corporate & Finance department and co-heads the Data Protection, Privacy & Cybersecurity Practice and the Competition Law & Regulatory Practice. He also heads the Telecommunications, Media and Technology ("TMT") Practice.

Chong Kin is a pioneer in the field of data protection in Singapore. His work in data protection, privacy and cybersecurity in Drew & Napier precedes the advent of Singapore's Personal Data Protection Act 2012 and Cybersecurity Act 2018. His expertise extends beyond general data protection law to sectoral frameworks, in particular, in the TMT and emerging AI sectors. Under Chong Kin's leadership, Drew & Napier has been recognised as one of the world's top 100 data law firms in *Global Data Review (GDR 100)*. Our TMT Practice Group has also been consistently ranked as the leading information technology, telecommunications, broadcasting and multimedia legal practice in Singapore.

His clients include data protection regulators, MNCs driving the data world, and many global technology clients. Chong Kin's private sector experience includes advising corporations on their data protection compliance programmes, policies and practices, data breach management and cross-border data transfers (including in relation to transfer impact assessments). Chong Kin and his team have also advised clients on sectoral data protection requirements for many years, including that under TMT, financial and healthcare sectoral laws.

Chong Kin established the Drew Data Protection and Cybersecurity Academy (<https://www.drewnapier.com/Data-Protection-Cybersecurity-Academy>) in 2020, a first of its kind which offers clients value-add services including training and external DPO services.

Chong Kin has consistently been cited as a leading lawyer by *Chambers Asia Pacific*, *Asia Pacific Legal 500*, *Asialaw Profiles*, *PLC Which Lawyer?*, *International Who's Who of Regulatory Communications Lawyers*, *Best Lawyers* and *Asialaw Leading Lawyers*.

Chong Kin has also been recognised as a Senior Accredited Specialist in Data and Digital Economy Law by the Singapore Academy of Law.

Drew & Napier LLC

10 Collyer Quay
10th Floor Ocean Financial Centre
Singapore 049315

Tel: +65 6531 4110
Email: chongkin.lim@drewnapier.com
LinkedIn: www.linkedin.com/in/chong-kin-lim



Anastasia Su-Anne Chen is a Director with the Corporate & Finance Department in Drew & Napier. Her key areas of practice are TMT, Data Protection, Privacy and Cybersecurity. Prior to joining the firm, Anastasia was Deputy Chief Counsel to Singapore's Personal Data Protection Commission (PDPC) and Info-communications Media Development Authority (IMDA) for over nine years. She was lead counsel for PDPC matters, IMDA procurement and intellectual property portfolios, as well as the legal advisor to IMDA's Data Administration Group. During her stint with the public sector, she advised on numerous significant national projects, including overseeing major revisions to the PDPA, which came into effect on 1 February 2021.

Anastasia has advised on a broad range of regulatory, compliance and commercial matters. Her extensive experience ranges from implementing data protection compliance programmes, developing playbooks and contractual clauses for novel areas such as AI (including for world-leading Generative AI platforms), as well as providing strategic advice on international data flows, the outsourcing of data processing and data incidents.

Anastasia has been recognised as a Senior Accredited Specialist in Data & Digital Economy Law by the Singapore Academy of Law. She has also received several accolades for her data and cybersecurity practice, with clients commending her deep industry and regulatory experience, ability to anticipate potential legal issues, and subject matter expertise especially when dealing with novel problems.

Anastasia speaks regularly at data protection conferences and corporate events on data privacy. She was also an editor for the *Personal Data Protection Digests* for Singapore and has penned several articles contributing to the jurisprudence on data protection in Singapore.

Drew & Napier LLC

10 Collyer Quay
10th Floor Ocean Financial Centre
Singapore 049315

Tel: +65 6531 4123
Email: anastasia.chen@drewnapier.com
LinkedIn: www.linkedin.com/in/anastasiasuannechen

Drew & Napier established a dedicated Data Protection, Privacy and Cybersecurity Practice (<https://www.drewnapier.com/Our-Expertise/Data-Protection-Privacy-Cybersecurity>) to leverage its unrivalled experience in data privacy and data and cyber governance and offer clients best-in-class solutions to address their legal and compliance needs in Singapore and across the region. Our expertise covers the full range of regulatory, commercial and global aspects of data protection and cybersecurity and, working in tandem with the Drew Data Protection & Cybersecurity Academy (<https://www.drewnapier.com/Academy>), we seek to address our clients' needs with an integrated and holistic approach.

The Practice Group is headed by Directors Lim Chong Kin and David N. Alfred and the team includes professionals with deep technical expertise and a solid understanding of corporate governance and business needs in relation to data protection and cybersecurity.

A distinguishing feature of the practice is our in-house expertise on cybersecurity engineering, headed by a senior cybersecurity and privacy

engineer, Albert Pichlmaier, who has more than 30 years of experience. This enables the team to deliver a holistic solution to clients on data protection and cybersecurity compliance.

Our experience in data protection, privacy and cybersecurity predates, and also extends beyond, Singapore's Personal Data Protection Act 2012 (PDPA) and Cybersecurity Act 2018.

www.drewnapier.com

 **DREW & NAPIER**

The **International Comparative Legal Guides** (ICLG) series brings key cross-border insights to legal practitioners worldwide, covering 58 practice areas.

Data Protection 2025 features four expert analysis chapters and 27 Q&A jurisdiction chapters covering key issues, including:

- Relevant Legislation and Competent Authorities
- Territorial and Material Scope
- Key Principles
- Individual Rights
- Children's Personal Data
- Registration Formalities and Prior Approval
- Appointment of a Data Protection Officer
- Appointment of Processors
- Marketing
- Cookies
- Restrictions on International Data Transfers
- Whistle-blower Hotlines
- CCTV
- Employee Monitoring
- Data Security and Data Breach
- Enforcement and Sanctions
- E-discovery/Disclosure to Foreign Law Enforcement Agencies
- Artificial Intelligence