International Comparative Legal Guides

Data Protection 2020

A practical cross-border insight into data protection law

Seventh Edition

Featuring contributions from:

Addison Bright Sloane
Anderson Mōri & Tomotsune
Chandler MHM Limited
Clyde & Co
DDPV Studio Legale
Deloitte Kosova Shpk
Deloitte Legal Shpk
D'LIGHT Law Group
DQ Advocates Limited
Drew & Napier LLC
Elzaburu S.L.P.
FABIAN PRIVACY LEGAL GmbH
Herbst Kinsky Rechtsanwälte GmbH
Homburger AG
Khaitan & Co LLP
King & Wood Mallesons
Koushos Korfiotis Papacharalambous LLC
Lee and Li, Attorneys-at-Law
Leśniewski Borkiewicz & Partners
LPS L@w
LYDIAN
Marval O'Farrell Mairal
Matheson
Mori Hamada & Matsumoto
Naschitz, Brandes, Amir & Co., Advocates
NEOVIAQ IP/ICT
Nyman Gibson Miralis
OLIVARES
Pellon de Lima Advogados
PPM Attorneys
Rothwell Figg
Semenov&Pevzner
SEOR Law Firm
SKW Schwarz Rechtsanwälte
SSEK Indonesian Legal Consultants
S. U. Khan Associates Corporate & Legal Consultants
Synch Advokatpartnerselskab
Templars
White & Case LLP
White & Case, s.r.o., advokátní kancelář
Wikborg Rein Advokatfirma AS

ICLG.com

Expert Chapters

Q&A Chapters

Q&A Chapters Continued

Singapore

Drew & Napier LLC

Lim Chong Kin

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The Personal Data Protection Act 2012 (No. 26 of 2012) ("**PDPA**") is the principal data protection legislation in Singapore. The PDPA establishes a general data protection law which applies to all private sector organisations.

Parts III to VI of the PDPA set out obligations of organisations in respect of the collection, use, disclosure, access, correction, care, protection, retention, and transfer of personal data (collectively, "**Data Protection Provisions**"); while Part IX 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 2014 ("**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 (Composition of Offences) Regulations 2013;
- the Personal Data Protection (Do Not Call Registry) Regulations 2013;
- the Personal Data Protection (Enforcement) Regulations 2014; and
- the Personal Data Protection (Appeal) Regulations 2015.

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 (Cap. 50A) 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 (No. 9 of 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 (Cap. 311A) ("**SCA**") regulates the bulk sending of unsolicited commercial electronic messages to email addresses or mobile telephone numbers, complementing the DNC Provisions of the PDPA. The DNC Provisions of the PDPA and the SCA are expected to be merged into a new Act dealing with unsolicited commercial electronic messages generally.

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 (Cap. 19) ("**Banking Act**") contains a number of banking secrecy provisions which govern customer information obtained by banks;
- the Telecoms Competition Code issued under the Telecommunications Act (Cap. 323) contains provisions governing the use of end-user service information by telecoms licensees; and
- the Private Hospitals and Medical Clinics Act (Cap. 248) and the licensing terms and conditions issued thereunder contain provisions addressing the confidentiality of medical information and the retention of medical records.

With regard to the financial sector, the Monetary Authority of Singapore ("**MAS**") is empowered under the Monetary Authority of Singapore Act (Cap. 186) and other sectoral legislation to issue directives and notices. Examples of MAS-issued regulatory instruments which are relevant to data protection include the 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 the law, 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 the Protection Obligation and the Retention Limitation Obligation (as defined below).
- "**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**"
  The PDPA does not expressly distinguish between specific categories of personal data. The term "sensitive personal data" is therefore 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 extent of the data protection obligations to which an organisation is subject. 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] SGPDPC 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 consider this to be an aggravating factor in calculating the level of the financial penalty to be imposed on the organisation.
- "**Data Breach**"
  The PDPA does not expressly define "data breach". However, the PDPC, in its Guide to Managing Data Breaches 2.0, refers to a "data breach" as "an incident exposing personal data in an organisation's possession or under its control to the risks of unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks". An organisation is required, under Section 24 of the PDPA, to protect personal data against such risks.

Other key definitions – please specify (e.g., "Pseudonymous Data", "Direct Personal Data", "Indirect Personal Data")

- "**Business Contact Information**" is defined as an individual's name, position name or title, business telephone number, business address, business electronic mail address or business fax number and any other similar information about the individual, not provided by the individual solely for his personal purposes.
  Organisations are not required to obtain consent before collecting, using or disclosing any business contact information, or to comply with any other obligation in the Data Protection Provisions in relation to business contact information.

3 Territorial Scope

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

The PDPA applies to all organisations which are not a public agency or acting on behalf of 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.

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 (see section 7 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 Second, Third or Fourth 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 – namely, the Purpose Limitation Obligation, the Accuracy Obligation, the Protection Obligation, and the Retention Limitation Obligation (as defined below) – make reference 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**").

Other key principles – please specify

- 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**").
- 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 unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks ("**Protection Obligation**") (see our response to section 15 below).
- 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 organisations provide a standard of protection to the transferred personal data that is comparable to the protection under the PDPA ("**Transfer Limitation Obligation**") (see our responses in section 11 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 data/copies of data**
  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 repetitious or systematic nature of the request;
  - 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.

- **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; and
  - a document related to a prosecution if all proceedings related to the prosecution have not been completed.

  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**

  Currently, this is not applicable in Singapore.

  As part of its review of the PDPA, the PDPC, on 22 May 2019, conducted a public consultation on a proposed Data Portability Obligation, which requires organisations to, at the request of the individual, provide the individual's data that is in the organisation's possession or under its control, to be transmitted to another organisation in a commonly used machine-readable format. On 20 January 2020, the PDPC issued its response to the feedback received and proposed, *inter alia*, to have the Data Portability Obligation come into effect in phases through the issuance of regulatory instruments, so that it can be tailored to the needs and readiness of the industry.

- **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 9.1 below).

- **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.

6 Registration Formalities and Prior Approval

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

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

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

This is not applicable in Singapore.

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

This is not applicable in Singapore.

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

This is not applicable in Singapore.

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

This is not applicable in Singapore.

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

This is not applicable in Singapore.

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

This is not applicable in Singapore.

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

This is not applicable in Singapore.

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

This is not applicable in Singapore.

6.10 Can the registration/notification be completed online?

This is not applicable in Singapore.

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

This is not applicable in Singapore.

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

This is not applicable in Singapore.

7 Appointment of a Data Protection Officer

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

The appointment of a Data Protection Officer ("**DPO**") 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) and 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.

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

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 of such amount not exceeding S$1 million as the PDPC sees fit.

For completeness, we note that the PDPC has actively enforced this requirement over the past year.

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

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.

7.4 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 conferred by that delegation on another individual. For the avoidance of doubt, the designated individual need not be an employee of the organisation.

7.5 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 would be 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 which a DPO needs, and to assist organisations in the hiring and training of data protection professionals.

7.6 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 when 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.

7.7 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 subscribe to the PDPC's *DPO Connect* newsletter in order to keep abreast of developments in the PDPA.

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

No. However, the business contact information of at least one DPO must be made available to the public.

8 Appointment of Processors

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

There is no strict requirement for an agreement between the organisation and data intermediary under the PDPA. 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*".

The 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. If there is no contract evidenced or made in writing with the data organisation, the data intermediary will need to comply with all the Data Protection Provisions in respect of the personal data that is processed on behalf of the data organisation.

Furthermore, where an organisation engages a data intermediary, the organisation is responsible for complying with the Transfer Limitation Obligation in respect of any overseas transfer of personal data (i.e. by the organisation to the overseas data intermediary, or by the data intermediary itself as part of the processing) (see section 11 below). To comply with the Transfer Limitation Obligation, the organisation may need to undertake appropriate due diligence and obtain assurances from the data intermediary, and/or ensure that the recipient is bound by legally enforceable obligations, which may include a contract fulfilling the requirements under the PDP Regulations.

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

As the organisation remains responsible for complying with the PDPA notwithstanding that a data intermediary is processing personal data on its behalf, it may be prudent for the organisation to 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.

If it is contemplated that there will be overseas transfers of personal data, the agreement may provide assurances to ensure that the personal data is 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 Transfer Limitation Obligation at section 11 below.

9 Marketing

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

The 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) verify against the relevant DNC Registry to confirm that the telephone number is not listed 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; and
(c) for voice calls, not conceal or withhold the calling line identity from the recipient.

In relation to the sending of unsolicited marketing communications in bulk by email or other electronic messages, 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 reflective of the message's content;
(d) a label "<ADV>" with a space before the title of the subject field or, in the absence of a title, 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.

9.2 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 Data Protection Provisions in the PDPA would likely not be applicable in those instances.

In specific 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 9.1 above) would similarly apply.

For completeness, from April to June 2018, the PDPC conducted a public consultation proposing to streamline the requirements under the DNC Provisions and the SCA. The Response to Feedback on the Public Consultation (issued 8 November 2018) stated that the PDPC intends to retain the current exclusion of B2B marketing messages from the DNC Provisions.

9.3 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 9.1 above.

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

Yes, if the recipient of the marketing messages is present in Singapore when the marketing message is accessed. With respect to the collection, use and disclosure of personal data for marketing purposes, the Data Protection Provisions of the PDPA apply to all organisations, whether or not 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, when the message is sent: (i) an individual who is physically present in Singapore; or (ii) an entity whose central management and control is 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.

9.5 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.

9.6 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] SGPDPC 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] SGPDPC 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 had provided their consent and were notified of the disclosure, and if so, obtain a sample of such consent and notification. 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.

9.7 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.

In relation to the DNC Registry:

(a) For breaches of the obligation to check the DNC Registry, the offender would be guilty of an offence and liable on conviction to a fine not exceeding S$10,000.

(b) For breaches of the obligation to provide clear and accurate information identifying the sender and the sender's contact details in the prescribed manner, the offender would be guilty of an offence and liable on conviction to a fine not exceeding S$10,000.

(c) For breaches of the obligation to provide the recipient with the calling line identity of the sender, the offender would be guilty of an offence and liable on conviction to a fine not exceeding S$10,000.

In appropriate cases, the PDPC may compound the offence for a sum of up to S$1,000. Whether composition is offered, and the amount of composition, will be decided by the PDPC based on the facts of each case.

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

10 Cookies

10.1 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.

Consent may also be reflected in the way a user configures his interaction with the Internet. If the individual configures his browser to accept certain cookies but rejects others, he may be found to have consented to the collection, use and disclosure of his personal data by the cookies that he has chosen to accept.

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

This is not applicable in Singapore.

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

To date, the PDPC has not issued any enforcement decisions specifically in relation to cookies.

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

This is not applicable in Singapore.

11 Restrictions on International Data Transfers

11.1 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 abroad to do so only in accordance with the requirements prescribed under the PDPA to ensure that the recipients provide a standard of protection to personal data so transferred that is comparable to the protection under the PDPA.

In particular, under the PDP Regulations, the transferring organisation must, before transferring the personal data outside of Singapore:

- take appropriate steps to ensure that the transferring organisation continues to comply with the Data Protection Provisions in respect of the personal data being transferred so long as such personal data remains in its possession or under its control; and
- take appropriate steps to ascertain whether, and to ensure that, the recipient is bound by legally enforceable obligations to provide the personal data transferred with a standard of protection comparable to that provided for by the PDPA.

For completeness, the PDP Regulations provide for certain prescribed situations whereby either or both of the above requirements are taken to be satisfied, e.g., where the personal data is publicly available in Singapore or where the personal data is data in transit.

"Legally enforceable obligations" is defined in the PDP Regulations to 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.

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.

11.2 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 8.1 and 8.2 above where there are any overseas transfers of personal data with respect to organisations engaging data intermediaries.

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

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

12 Whistle-blower Hotlines

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

The PDPA does not 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, and it is reasonable to expect that seeking the consent of the individual would compromise the availability or the accuracy of the personal data. 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.

12.2 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.

13 CCTV

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

The 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.

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.

13.2 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.

14 Employee Monitoring

14.1 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 overlaps with the employer's obligations under the PDPA, such monitoring will fall under the regulation of the Data Protection Provisions.

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

Before collecting, using or disclosing the personal data (which would include CCTV images/footage of such employees and the other data collected by the employer pursuant to their employee monitoring activities, to the extent that the employees can be identified from such data alone or with other information to which the organisation is likely to have access) of their employees, employers are generally required to provide suitable notices and obtain consent.

An exception to this requirement under the PDPA is where personal data is collected by the employer and the collection is reasonable for the purpose of managing or terminating an employment relationship between the employer and employee.

Due to the inherent uncertainty of the ambit of this exception, it is common for employers to include related clauses in their personal data protection policies, employment handbook or employment agreements to obtain express consent from their employees prior to the commencement of employee monitoring or using CCTV surveillance. It is also not unusual for organisations to provide prominent notices at the entrances of their premises to alert visitors that their premises are monitored by CCTV. Such notices should state the purpose of the CCTV.

14.3 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 Data Security and Data Breach

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

Yes, 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.

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

There is currently no mandatory requirement under the PDPA for organisations to report data breaches to the PDPC. However, the PDPC recommends that organisations provide notification to the PDPC as soon as possible of any data breaches that might cause public concern, or where there is a risk of harm to a group of affected individuals, or where the data breach involves sensitive personal data.

The PDPC has indicated through public statements, including a public consultation issued on 27 July 2017, that it intends to introduce a mandatory data breach notification regime. However, this proposed regime has yet to take effect.

To prepare organisations for the change, the PDPC has published a Guide to Managing Data Breaches 2.0 (issued 22 May 2019) ("**Data Breach Guide**"), which provides guidance to organisations with respect to the actions to be taken after a data breach, including reporting the breach.

Requirement to Notify

The Data Breach Guide states that organisations should notify the PDPC of a data breach that is:

- likely to result in significant harm to or impact on the individuals to whom the data relates; or
- of a significant scale (i.e. the data breach involves personal data of 500 or more individuals).

The PDPC has clarified that data intermediaries need not notify the PDPC or affected individuals of a data breach. Each data intermediary should instead inform its client, the organisation, of a potential or confirmed data breach without undue delay (i.e. within 24 hours).

Organisations should consider alerting the police if they suspect the involvement of criminal activity (e.g. hacking, theft or unauthorised system access by an employee), and preserving

evidence for investigation. Organisations may also wish to alert the Cyber Security Agency of Singapore through the Singapore Computer Emergency Response Team ("**SingCERT**") in the case of cyberattacks.

Timeframe for Notification

With regard to the timeframe for reporting, the Data Breach Guide states that organisations are to notify the PDPC as soon as practicable, but no later than 72 hours after establishing that the data breach fulfils the criteria as stated above.

Details of Notification

The notification to the PDPC should include information such as:

- extent of the data breach;
- type(s) and volume of personal data involved;
- cause or suspected cause of the breach;
- whether the breach has been rectified;
- measures and processes that the organisation had put in place at the time of the breach;
- information on whether individuals affected by the data breach were notified and if not, when the organisation intends to do so; and
- contact details of person(s) whom the PDPC could contact for further information or clarification.

Where the specific information of the data breach is not yet available, organisations should send an interim notification comprising a brief description of the data breach.

Effect of Notification

The Data Breach Guide also provides that notifications or lack thereof will affect the PDPC's decision as to whether an organisation has reasonably protected the personal data in its possession or under its control.

Furthermore, according to the Enforcement Guidelines, the fact that an organisation has voluntarily notified the PDPC of a data breach as soon as it learned of the breach, and cooperated with the PDPC in its investigations, may be a mitigating factor that the PDPC will take into account when calculating the financial penalty.

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

There is currently no mandatory requirement under the PDPA for organisations to notify individuals of data breaches. However, an organisation may need to provide such notification to individuals pursuant to its other legal or contractual obligations.

In its Data Breach Guide, the PDPC recommended that organisations notify individuals affected by a data breach as a matter of best practice. Such notification should also be provided to parents or guardians of young children whose personal data has been compromised, third parties such as banks, credit card companies or the police (where relevant).

In terms of timing, affected individuals whose data has been compromised should be notified as soon as practicable.

The notification to affected individuals (or, where appropriate, the parents or guardians of young children) may include the following information:

- how and when the data breach occurred;
- the types of personal data involved in the data breach;
- what the organisation has done or will be doing in response to the risks brought about by the data breach;
- specific facts on the data breach where applicable, and actions individuals can take to prevent that data from being misused or abused;
- contact details and how affected individuals can reach the organisation for further information or assistance (e.g. helpline numbers, email addresses or websites); and/or
- where applicable, what type of harm/impact the individual may suffer from the compromised data.

As set out in the Enforcement Guidelines, the following are considered by the PDPC to be mitigating factors:

- the organisation took immediate steps to notify affected individuals of the breach and reduce the damage caused by a breach (such as informing individuals of steps they can take to mitigate risk); and
- the organisation has engaged the individual in a meaningful manner and has voluntarily offered a remedy to the individual, and that individual has accepted the remedy.

15.4 What are the maximum penalties for data security breaches?

The PDPC has discretion to issue such remedial directions as it sees fit, including a direction to require payment of a financial penalty of up to S$1 million.

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.

16 Enforcement and Sanctions

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

Investigatory/Enforcement Power	Civil/Administrative Sanction	Criminal Sanction
Power to require documents or information.	Not applicable.	Individuals may be liable to a fine of up to S$10,000 or imprisonment for a term of up to 12 months, or both, whereas organisations may be liable to a fine of up to S$100,000 for providing any false or misleading statements or information to the PDPC.

Investigatory/Enforcement Power	Civil/Administrative Sanction	Criminal Sanction
Power to enter premises with or without a court-issued search warrant.	Not applicable.	Individuals may be liable to a fine of up to S$10,000 or imprisonment for a term of up to 12 months, or both, whereas organisations may be liable to a fine of up to S$100,000 for obstructing or hindering the PDPC.
Power to review, on application of a complainant: (i) refusals to provide access to personal data requested by the complainant under the PDPA or a failure to provide such access within a reasonable time; (ii) a fee required from the complainant by an organisation in relation to a request by the complainant under the PDPA; or (iii) refusals to correct personal data in accordance with a request by the complainant under the PDPA.	The PDPC may: (i) confirm the refusal to provide access to or correct the personal data (as the case may be) and 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.	Not applicable.
Power to give directions.	The PDPC may issue such directions as it thinks fit in the circumstances to ensure compliance by an organisation with the Data Protection Provisions under Parts III to VI of the PDPA. These include 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 of up to S$1 million.	Not applicable.

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

The 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.

16.3 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.

Over the past year (2019), the PDPC has published more than 50 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 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$9,000 was imposed on Singapore Telecommunications Limited ("**SingTel**") for a breach of the Protection Obligation. The PDPC found that SingTel failed to carry out more thoroughly scoped tests of its mobile application and systems used for migrating subscriber records, which resulted in the personal data of 750 individuals put at risk of unauthorised access.
- A financial penalty of S$26,000 was imposed on SPH Magazines Pte Ltd ("**SPH**") for a breach of the Protection Obligation. The PDPC found that SPH failed to implement and enforce reasonable password security requirements on the senior moderator accounts and to conduct security testing on its forum website (which it operates, hosts and maintains). The data breach was the result of a hacker compromising the senior moderator account and subjecting the user profiles of 685,393 forum members to the risk of unauthorised access.
- Directions, including a financial penalty of S$20,000, were issued to the Society of Tourist Guides (Singapore) ("**Society**") for a breach of the Protection and Accountability Obligations. The PDPC found that the Society, in engaging an IT vendor to develop its website, had failed to make data protection part of its contractual terms. In particular, the Society failed to specify any security requirements to its IT vendor with respect to the storage and protection of personal data collected through the website (e.g. implementing access controls), in breach of the Protection Obligation. In addition, it was discovered that the Society had never conducted security testing on the website since its launch in 2018. Finally, the Society was also found to have breached the Accountability Obligation for failing to appoint a DPO and to develop and implement data protection policies and practices.

16.4 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 *Re Cigna Europe Insurance Company S.A.-N.V.* [2019] SGPDPC 18).

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 Asia-Pacific Economic Cooperation ("**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.

17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

17.1 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 11 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.

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

The PDPC has not issued any specific guidance yet in relation to foreign e-discovery requests or requests for disclosure from foreign law enforcement agencies.

18 Trends and Developments

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

Breaches of the Protection Obligation under the PDPA continue to constitute the majority of enforcement decisions issued by the PDPC, with 51 out of 61 cases over the past 12 months involving the Protection Obligation. Instances where businesses have been found to have inadequate privacy policies in place have decreased, although there were still five cases where businesses were found to have inadequate privacy policies.

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

APEC CBPR

On 20 February 2018, Singapore became the sixth APEC economy to participate in the APEC Cross-Border Privacy Rules ("**CBPR**") system. Singapore also became the second APEC economy to participate in the APEC Privacy Recognition for Processors ("**PRP**") system. On 17 July 2019, the IMDA announced that it had been appointed as Singapore's Accountability Agent for the APEC CBPR and PRP systems, and henceforth, organisations in Singapore can now be certified under both systems for accountable data transfers across borders to other certified organisations.

Data Protection Trustmark Certification Scheme

On 9 January 2019, the IMDA launched the Data Protection Trustmark ("**DPTM**") certification scheme for the CBPR and PRP systems, which was developed by the PDPC. The certification establishes a robust data governance standard to help businesses increase their competitive advantage and build trust with their customers. The certification requirements are based on parameters including relevance to the PDPA, international standards (e.g. APEC CBPR/PRP requirements) and industry best practices.

Model Artificial Intelligence Governance Framework

On 23 January 2019, the PDPC issued a Model Artificial Intelligence Governance Framework ("**Model AI Framework**") for public consultation and pilot adoption. This accountability-based framework helps chart the language and frame the discussions around harnessing AI in a responsible way. On 21 January 2020, the PDPC released the second edition of the Model AI Framework, accompanied by the Implementation and Self-Assessment Guide for Organisations ("**ISAGO**") and the Compendium of Use Cases. The former is aimed at helping organisations assess the alignment of their AI governance practices with the Model AI Framework, while the latter provides case studies as to how local and international organisations across different sectors and sizes have implemented or aligned their AI governance practices with all sections of the Model AI Framework.

Guide on Active Enforcement Released

On 22 May 2019, the PDPC published a Guide on Active Enforcement, which articulates the PDPC's new approach in deploying its enforcement powers. Notably, the Guide introduces two other enforcement options – undertakings and expedited decisions – which may be pursued *in lieu* of a full investigation. The undertaking process includes a written agreement between the organisation involved and the PDPC, in which the organisation voluntarily commits to remedy the breaches and take steps to prevent recurrence. An undertaking may be available if it achieves a similar or better enforcement outcome for the PDPC, or where the organisation can show that it has accountable data privacy practices in place, e.g. a DPTM certification, and that it has an effective remediation plan which it is prepared to implement. With respect to the latter, the PDPC may consider an expedited decision if there is an up-front admission of liability by the organisation involved for its role in the cause of the breach.

Lim Chong Kin heads Drew & Napier's Technology, Media and Telecommunications Practice Group, and is co-head of the firm's Data Protection, Privacy & Cyber-security Practice.

Under Chong Kin's leadership, these Practices are consistently ranked as the leading practices in Singapore. His clients include the telecoms and media regulators, global carriers, technology market leaders, global broadcasters and content providers.

Chong Kin has been an external legal and regulatory advisor for the Personal Data Protection Commission of Singapore since 2013, and he played a key role in the liberalisation of Singapore's telecoms, media and postal sectors, where he drafted the competition frameworks.

Chong Kin is highly regarded by his peers, clients and rivals alike for his expertise, and is consistently recommended as a leading lawyer by major international legal publications such as *Chambers Asia-Pacific*, *The Legal 500 Asia Pacific*, *Who's Who Legal*, *The Guide to the World's Leading Competition & Antitrust Lawyers/Economists*, *Global Competition Review*, *Practical Law Company – Which Lawyer?*, *Asialaw Profiles* and *Best Lawyers*.

Drew & Napier LLC
10 Collyer Quay
10th Floor, Ocean Financial Centre
Singapore 049315

Tel: +65 6531 4110
Email: chongkin.lim@drewnapier.com
URL: www.drewnapier.com

Drew & Napier LLC has provided exceptional legal advice and representation to discerning clients since 1889 and is one of the leading and largest law firms in Singapore.

The calibre of our work is acknowledged internationally at the highest levels of government and industry. Our lawyers and senior counsel are the preferred choice when the stakes are high and the issues complex.

The firm possesses unparalleled transactional, licensing and regulatory experience in data protection law as well as the technology, media and telecommunications, and postal sectors in Singapore, which is vested in its Telecommunications, Media and Technology Practice Group, led by Lim Chong Kin.

Drew & Napier assists clients in a wide range of data protection matters including: data protection review; training; compliance audits; and advisory.

Since 2013, the firm has been appointed by the Personal Data Protection Commission as its external legal and regulatory advisor, which speaks volumes to its proven ability to deliver effective, timely and commercially relevant solutions to its clients.

www.drewnapier.com

DREW & NAPIER

ICLG.com

Current titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Cybersecurity
Data Protection
Derivatives
Designs
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Family Law
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Outsourcing
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

@ICLG_GLG

The International Comparative Legal Guides are published by:

global legal group