COUNTRY COMPARATIVE GUIDES 2024

The Legal 500 Country Comparative Guides

Singapore

DATA PROTECTION & CYBERSECURITY

Contributor

Drew & Napier LLC

Lim Chong Kin

Managing Director, Corporate & Finance | chongkin.lim@drewnapier.com

Anastasia Su-Anne Chen

Director, Corporate & Finance | anastasia.chen@drewnapier.com

This country-specific Q&A provides an overview of data protection & cybersecurity laws and regulations applicable in Singapore.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

SINGAPORE
DATA PROTECTION & CYBERSECURITY

1. Please provide an overview of the legal and regulatory framework governing data protection, privacy and cybersecurity in your jurisdiction (e.g., a summary of the key laws; who is covered by them; what sectors, activities or data do they regulate; and who enforces the relevant laws).

The Personal Data Protection Act 2012 (2020 Revised Edition) ("**PDPA**") is the principal data protection legislation in Singapore which governs the collection, use and disclosure of individuals' personal data by organisations. In terms of application, the PDPA applies to all private sector organisations, whether or not (a) formed or recognised under the laws of Singapore, or (b) resident or having an office or a place of business in Singapore.

There are two main sets of provisions under the PDPA: Parts 3 to 6B of the PDPA set out obligations of organisations in respect of the collection, use, disclosure, access, correction, care, protection, retention, and cross-border transfer of personal data (collectively, "**Data Protection Provisions**"); while Parts 9 and 9A of the PDPA set 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**").

The PDPA and its subsidiary legislation, including the Personal Data Protection Regulations 2021 ("**PDP Regulations**"), are administered and enforced by the Personal Data Protection Commission ("**PDPC**"). Over the years, the PDPC has issued a number of advisory guidelines and guides which aim to provide greater clarity on the interpretation of the provisions of the PDPA.

The Personal Data Protection (Amendment) Act 2020 was passed on 2 November 2020 ("**Amendment Act**"). This introduced a number of changes to the PDPA, including an expansion of the concept of deemed consent (deemed consent by notification and deemed consent by contractual necessity), the introduction of new exceptions to consent (legitimate interests exception and business improvement exception), the introduction of a mandatory data breach notification regime, an enhanced financial penalty regime, new offences for individuals, and provisions on data portability. Most of the changes under the Amendment Act came into effect on 1 February 2021. On 1 October 2022, the Amendment Act provisions relating to enhanced financial provisions came into effect. The provisions relating to data portability will only come into force at a later date.

Sectoral Laws

The PDPA sets the baseline for data protection and operates concurrently with sector-specific laws and regulations, which imposes additional data protection and cybersecurity requirements in relation to regulated entities.

We set out some examples of sector-specific regulations below:

a. the Healthcare Services Act 2020 (No. 3 of 2020) ("**HCSA**"), as well as the regulations and licensing conditions issued thereunder address the confidentiality and retention of medical records;
b. the Code of Practice for Competition in the Provision of Telecommunication Services 2012 ("**Telecom Competition Code**", "**TCC**") issued under the Telecommunications Act 1999 (2020 Revised Edition) governs the use of end-user service information by telecoms licensees; and
c. the Banking Act 1970 (2020 Revised Edition) ("**Banking Act**") contains a number of banking secrecy provisions which govern customer information obtained by banks.

The above legislations are administered and enforced by

the relevant sector regulators, namely, the Ministry of Health ("**MOH**"), the Info-communications Media Development Authority ("**IMDA**"), and the Monetary Authority of Singapore ("**MAS**").

Aside from the above sector-specific regulations, we also point to the Cybersecurity Act 2018 (No. 9 of 2018) ("**Cybersecurity Act**") which requires owners and operators of critical information infrastructure ("**CII**") to comply with cybersecurity policies and standards, conduct audits and risk assessments, and implement incident reporting measures. The Cybersecurity Act also creates a framework for the licensing and regulation of certain types of cybersecurity services. The Chief Executive of the Cybersecurity Agency of Singapore ("**CSA**") administers the Cybersecurity Act as the Commissioner of Cybersecurity.

2. Are there any expected changes in the data protection, privacy or cybersecurity landscape in 2024–2025 (e.g., new laws or regulations coming into effect, enforcement of such laws and regulations, expected regulations or amendments (together, "data protection laws"))?

On 3 April 2024, the first reading of the Cybersecurity (Amendment) Bill ("**Amendment Bill**") took place in Parliament. Under the Amendment Bill, existing provisions relating to the cybersecurity of CII owners would be updated and the CSA's oversight would be widened to cover the cybersecurity of systems of temporary cybersecurity concern ("**STCCs**"). Two new classes of regulated entities, entities of special cybersecurity interest ("**ESCI**") and foundational digital infrastructure ("**FDI**"), which will be subject to a light-touch regulatory treatment, were also introduced. Companies that provide foundational digital infrastructure services (such as cloud computing service providers and data centres) would also be required to adhere to cybersecurity codes and standards of practice, and be subject to cybersecurity incident reporting requirements, though not at the level of CII owners.

3. Are there any registration or licensing requirements for entities covered by these data protection laws, and if so what are the requirements? Are there any exemptions?

Under the PDPA, there is currently no requirement for organisations to register with or obtain any licence from the PDPC. However, the PDPC does encourage organisations to inform the PDPC of their Data Protection Officer's ("**DPO**") contact details as this will help DPOs keep abreast of relevant personal data protection developments in Singapore.

Sectoral laws and regulations apply to the relevant licensed or otherwise regulated organisations. Registration or licensing requirements and the exemptions available depend on the specific organisation.

Under the Cybersecurity Act, cybersecurity service providers must obtain a licence. Licensable cybersecurity services are managed security operations centre monitoring service and penetration testing service (Second Schedule to the Cybersecurity Act).

4. How do these data protection laws define "personal data," "personal information," "personally identifiable information" or any equivalent term in such legislation (collectively, "personal data") versus special category or sensitive personal data? What other key definitions are set forth in the data protection laws in your jurisdiction?

Personal Data

The term "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.

The PDPA does not distinguish between specific categories of personal data, and the term "sensitive personal data" is not defined within the PDPA. Notwithstanding, the sensitivity of the personal data in question could, in practice, affect the regulatory outcome in relation to a contravention of the relevant provision (see Question 8 below).

Other Key Definitions

"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 comply with any other obligation in the

Data Protection Provisions in relation to business contact information, unless expressly stated in the PDPA.

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.*"

The PDPA makes a distinction between an "organisation" and a "data intermediary", the latter of 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*".

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, the Retention Limitation Obligation and some aspects of the Data Breach Notification Obligation under the PDPA.

5. What are the principles related to the general processing of personal data in your jurisdiction? For example, must a covered entity establish a legal basis for processing personal data, or must personal data only be kept for a certain period? Please outline any such principles or "fair information practice principles" in detail.

All organisations that collect, use or disclose personal data are required to comply with the Data Protection Provisions under the PDPA.

The data protection obligations that are presently in force comprise the following:

a. Consent Obligation (Sections 13 to 17 of the PDPA): Subject to certain exceptions, an individual's consent is required before an organisation is allowed to collect, use or disclose his/her personal data for a specific purpose.
b. Purpose Limitation Obligation (Section 18 of the PDPA): An organisation may only collect, use or disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances, and provide notification to the individual concerned.
c. Notification Obligation (Section 20 of the PDPA): An organisation is required to notify the individual of the purpose(s) for which it intends to collect, use or disclose his/her personal data on or before such collection, use or disclosure.
d. Access and Correction Obligations (Sections 21 and 22 of the PDPA): Subject to certain exceptions as specified in the PDPA, an organisation must allow an individual to access and correct his/her personal data in its possession or under its control upon request in accordance with the requirements in Part 2 of the PDP Regulations. In addition, it must provide the individual with information about the ways in which the personal data may have been used or disclosed during the past year.
e. Accuracy Obligation (Section 23 of the PDPA): An organisation must make a reasonable effort to ensure that personal data collected by it is accurate and complete, if it is likely to use such personal data to make a decision that affects the individual concerned, or disclose such personal data to another organisation.
f. Protection Obligation (Section 24 of the PDPA): An organisation will be required to protect personal data in its possession or under its control by making reasonable security arrangements to prevent (a) unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks, and (b) the loss of any storage medium or device on which personal data is stored.
g. Retention Limitation Obligation (Section 25 of the PDPA): An organisation is required to 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 the retention of such personal data no longer serves the purpose for which it was collected, and is no longer necessary for legal or business purposes.
h. Transfer Limitation Obligation (Section 26 of the PDPA): An organisation must not transfer personal data to a country or territory outside Singapore except in accordance with requirements prescribed under the PDPA and Part 3 of the PDP Regulations to ensure that the overseas recipient provides a standard of protection to the transferred personal data that is comparable to that under the PDPA.
i. Accountability Obligation (Sections 11 and 12 of the PDPA): An organisation must develop and implement policies and practices that are necessary for it to meet its obligations under the PDPA, and to make information about such policies and practices publicly available.

The organisation is also required to communicate to its staff information about its personal data protection policies and practices. The organisation is also required to designate one or more individuals (i.e., the DPO) to be responsible for ensuring that it complies with the PDPA.

j. Data Breach Notification Obligation (Sections 26A to 26E of the PDPA): An organisation must assess a data breach that affects personal data in its possession or under its control, and is required to notify the PDPC if the data breach results in, or is likely to result in, significant harm to individuals or if the data breach is of a significant scale. Further, if the data breach results in, or is likely to result in, significant harm, an organisation is required to notify the affected individuals (subject to certain exceptions).

There is another data protection obligation that was introduced in the Amendment Act, namely, the Data Portability Obligation. Under the Data Portability Obligation, an organisation, upon receiving a data porting request from an individual, must transmit the applicable data specified in the data porting request to the organisation specified in the request, in accordance with any prescribed requirements, such as requirements relating to technical, user experience, and consumer protection matters. As mentioned above, the data portability provisions will only come into effect at a later date, which has yet to be announced.

6. Are there any circumstances for which consent is required or typically obtained in connection with the general processing of personal data?

The Consent Obligation requires that an organisation obtain the consent (either express or deemed) from an individual before collecting, using, or disclosing his personal data for any purpose, unless an exception in the First or Second Schedules to the PDPA applies or it is otherwise authorised by written law. Therefore, in Singapore, consent is often relied on by organisations for processing personal data, especially of their consumers.

Under the PDPA, organisations that are relying on consent to collect, use and disclose personal data are required to notify the individuals of the purposes for such collection, use and disclosure in accordance with the Notification Obligation.

Furthermore, under the PDPA, such consent may be invalid where:

a. the organisation, as a condition of providing the product or service, requires the individual to consent to the collection, use or disclosure of his personal data beyond what is reasonable to provide the product or service; or
b. the organisation obtains consent by providing false or misleading information or using misleading and deceptive practices.

7. What are the rules relating to the form, content and administration of such consent? For instance, can consent be implied, incorporated into a broader document (such as a terms of service) or bundled with other matters (such as consents for multiple processing operations)?

In this regard, the PDPA does not expressly prescribe any specific means by which the organisation is to obtain consent, or the specific manner or form in which an organisation is to inform an individual of the purposes.

The Advisory Guidelines on Key Concepts in the PDPA (revised 16 May 2022) ("**Key Concept Guidelines**") state that organisations should determine the best way of notifying individuals such that they are provided with sufficient information to understand the purposes for which their personal data will be collected, used or disclosed.

Where an organisation intends to use or disclose personal data which has not been previously informed at the time of initial collection (i.e., where an organisation intends to use or disclose the personal data for new purposes), it must inform the individual of the new purposes of use or disclosure and obtain consent before the use or disclosure of the personal data for that purpose (Section 20(1)(b) of the PDPA).

While the PDPA does not set out rules specifically regarding the issue of obtaining consent through incorporation into a broader document such as a terms of use / service or obtaining consent for multiple matters, an organisation must ensure that it provides reasonable notice of its purposes. In particular, the PDPA contains a general obligation that an organisation must consider what a reasonable person would consider appropriate when complying with the other obligations in the PDPA such as the Notification and Consent Obligations.

Consent should be in writing or recorded in a manner that is accessible for future reference (except where

consent is deemed as described below). The PDPC recommends that organisations obtain consent from an individual through a positive action of the individual (i.e. "opt-in" consent). In the event that an organisation intends to adopt the "opt-out" approach in seeking consent, there may be a risk that the organisation may not have satisfied the Notification and Consent Obligations.

Deemed Consent

Sections 15 and 15A of the PDPA provide for three specific types of circumstances where consent may be deemed: (a) deemed consent by conduct; (b) deemed consent by contractual necessity; and (c) deemed consent by notification.

(A) Deemed consent by conduct

Deemed consent by conduct is where the individual voluntarily provides their personal data to the organisation and it is reasonable for them to do so (Section 15(1) of the PDPA). However, the purposes of collection, use or disclosure are limited to those that are objectively obvious and reasonably appropriate from the surrounding circumstances. Consent is deemed to be given to the extent that the individual intended to provide his/her personal data and took the action required for the data to be collected by the organisation (Key Concept Guidelines).

(B) Deemed consent by contractual necessity

Where an individual provides his/her personal data to one organisation A with a view to entering into a contract with A or in relation to a contract he/she has entered into with A, deemed consent by contractual necessity covers the situation where it is reasonably necessary for A to disclose the personal data to another organisation B for the conclusion or performance of the contract between the individual and A respectively (Sections 15(3) and 15(6) of the PDPA). This extends to subsequent downstream disclosures by B to other organisations, where such disclosure and collection are reasonably necessary to fulfil the contract between the individual and A.

(C) Deemed consent by notification

An individual may be deemed to have consented to the collection, use or disclosure of personal data for a purpose that he/she had been notified of, and he/she has not taken any action to opt out (Section 15A of the PDPA). An organisation must satisfy the following requirements in order to rely on deemed consent by notification: (a) conduct an assessment to determine that the proposed collection, use or disclosure of personal data is not likely to have an adverse effect on the individual; (b) take reasonable steps to ensure that the following information are brought to the individual's attention – (i) the organisation's intention to collect, use or disclose the personal data; (ii) the purpose of such collection, use or disclosure; and (iii) a reasonable period within which, and a reasonable manner by which, an individual can opt out; and (c) retain a copy of the assessment during the period that the organisation is relying on this Section 15A and provide a reasonable opt-out period.

8. What special requirements, if any, are required for processing sensitive personal data? Are any categories of personal data prohibited from collection or disclosure?

Sensitive Personal Data

The PDPA does not expressly define "sensitive personal data", nor does it prescribe any special requirements for the processing of "sensitive personal data".

Nonetheless, a number of the Data Protection Provisions adopt a standard of reasonableness, and thus, the sensitivity of the personal data in question could, in practice, affect the position which PDPC takes with respect to whether there is a contravention and the directions issued for such a contravention (for instance, the quantum of the financial penalty imposed).

Specifically, in relation to the Protection Obligation, the PDPC has taken the position in several enforcement decisions that an organisation has to implement reasonable security arrangements that commensurate with the sensitivity (and volume) of the data in question. Therefore, a higher standard of protection is required for personal data that is more sensitive in nature, such as financial or medical information, personal data of minors, and national identification numbers (see *Re Aviva Ltd* [2017] SGPDPC 14).

We further highlight that the Personal Data Protection (Notification of Data Breaches) Regulations 2021 provide for certain prescribed categories or classes of personal data that would be deemed to cause significant harm to an individual in the event of a data breach.

National Registration Identity Card ("**NRIC**") and Other National Identification Numbers

The PDPA also does not outright prohibit the collection of any type of personal data. However, the PDPC's Advisory Guidelines on the PDPA for NRIC and other National Identification Numbers (issued 31 August 2018) ("**NRIC Guidelines**") states that organisations are generally not

allowed to collect, use or disclose NRIC numbers (or copies of NRIC), unless such collection, use or disclosure:

a. is required under the law (or an exception under the PDPA applies); or
b. is necessary to accurately establish or verify the identities of the individuals to a high degree of fidelity.

Generally, the requirements in the NRIC Guidelines apply to other national identification numbers such as birth certificate numbers, Foreign Identification Numbers, work permit numbers, passport numbers.

9. How do the data protection laws in your jurisdiction address health data?

The provisions of the PDPA set a baseline standard of protection across all private organisations, including those in the healthcare sector. Nevertheless, as stated in Question 1, there are sectoral laws that have specific requirements in relation to health data. In particular, the HCSA, the Healthcare Services (General) Regulations 2021 as well as the licensing conditions thereunder contain provisions which address the confidentiality and retention of medical records.

10. Do the data protection laws in your jurisdiction include any derogations, exclusions or limitations other than those already described? If so, please describe the relevant provisions.

General Exceptions under the PDPA

Broadly, with respect to the application of the Data Protection Provisions, certain categories of "organisations" are excluded from the application of the PDPA, specifically:

a. individuals acting in a personal or domestic capacity;
b. employees acting in the course of their employment with an organisation;
c. public agencies; and
d. any other organisations or personal data, or classes of organisations or personal data, prescribed under the PDPA or its subsidiary legislation.

The PDPA does not apply to, or applies in a limited extent to, certain types of personal data. For example, the Data Protection Provisions do not apply to business contact information; or to personal data that has been contained in a record that has been in existence for at least 100 years.

In relation to personal data pertaining to deceased individuals, organisations will be subject to a limited scope of obligations, i.e. organisation need to comply only with the Protection Obligation and the requirements relating to disclosure of personal data, and only for 10 years from the deceased's date of death.

Exceptions to Specific Provisions

There are also exceptions with respect to specific Data Protection Provisions. For instance, as stated above, an organisation does not need to obtain consent for the collection, use or disclosure of personal data if an exception under the First or Second Schedules to the PDPA applies.

Some of these exceptions in the First or Second Schedules to the PDPA include where the collection, use or disclosure of personal data is necessary in the national interest; is necessary to respond to an emergency that threatens the life, health or safety of the individual; is publicly available; is necessary for evaluative purposes; is necessary for any investigation or proceedings; is reasonable for the purpose of managing or terminating an employment relationship, etc.

In relation to the Access Obligation, 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. There are also further exceptions under Section 21(3) of the PDPA.

Similarly, in relation to the Correction Obligation, 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. In addition, Section 22(6) of the PDPA clarifies that an organisation is not required to correct or otherwise alter an opinion.

11. Do the data protection laws in your jurisdiction address children's and teenagers' personal data? If so, please describe how.

The PDPA does not contain specific provisions that address the collection, use and disclosure of children's and teenagers' personal data.

Nonetheless, the PDPC has, in its Advisory Guidelines on the PDPA for Selected Topics (revised 17 May 2022) ("**Selected Topics Guidelines**"), provided guidance for

data activities in relation to minors (i.e. individuals who are less than 21 years of age).

With respect to consent, the PDPC provides that a minor who is at least 13 years old would typically have sufficient understanding to be able to consent on his own behalf for the purposes of the PDPA. Notwithstanding, if an organisation has reason to believe, or it can be shown, that a minor does not have sufficient understanding, the organisation should obtain consent from someone who can legally provide consent on the minor's behalf (e.g., parent or legal guardian).

The Selected Topics Guidelines also encourages organisations to put in place additional security measures with respect to the collection, use and disclosure of personal data of minors, for example, taking extra steps to verify the accuracy of personal data about a minor, especially where such inaccuracy may have severe consequences for the minor.

12. Do the data protection laws in your jurisdiction address online safety? Are there any additional legislative regimes that address online safety not captured above? If so, please describe.

The PDPA and Cybersecurity Act does not address online safety.

However, the Online Safety (Miscellaneous Amendments) Act, which took effect on 1 February 2023, introduced a new part to the Broadcasting Act 1994 ("**Broadcasting Act**") to tackle harmful content on online services accessible to Singapore users. It empowers the IMDA to designate social media services ("**SMSs**") with significant reach or impact in Singapore to comply with online codes of practice such as the Code of Practice for Online Safety ("**Online Safety Code**") (which was took effect on 18 July 2023). The designated SMSs are Facebook, HadwareZone, Instagram, TikTok, X, and YouTube.

The Online Safety Code seeks to enhance online user safety, particularly for children, and curb the harm of harmful content on SMSs. SMSes are required to implement measures such as measures minimise end-users' exposure to harmful content by requiring designated SMSs to put systems and processes in place to curb the spread of harmful content on their services, apply age appropriate policies to accounts belonging to children, and put in place tools for parents or guardians to manage the content that their children see and/or their experiences. The categories of harmful content covered by the Online Safety Code are:

- sexual content;
- violent content;
- suicide and self-harm content;
- cyberbullying content;
- content endangering public health; and
- content facilitating vice and organised crime.

13. Is there any regulator in your jurisdiction with oversight of children's and teenagers' personal data, or online safety in general? If so, please describe, including any enforcement powers. If this regulator is not the data protection regulator, how do those two regulatory bodies work together?

Personal data, including that of children and teenagers, is regulated by the PDPC. The PDPC's enforcement powers may be broadly categorised into powers relating to: alternative dispute resolutions, reviews, investigations, voluntary undertakings, directions and written notice to pay financial penalties.

Alternative dispute resolution

If the PDPC is of the opinion that any complaint by an individual against an organisation may more appropriately be resolved by mediation, the PDPC may, without the consent of the complainant and the organisation, refer the matter to mediation under a dispute resolution scheme (Section 48G of the PDPA).

Review refusals to provide access of or to correct personal data as requested

The PDPC has the power to conduct a review with respect to refusals to provide access to or correct personal data, fees in relation to such requests, or failure to provide access or correction within a reasonable time (Section 48H of the PDPA).

Investigations

The PDPC may, upon complaint or of its own motion, conduct investigations to determine whether an organisation (or person) is complying with the PDPA, among others (Section 50 of the PDPA). Its powers of investigation include the power to require documents or information, and to enter premises with or without warrant (Ninth Schedule to the PDPA).

Voluntary undertakings

The PDPC may accept a written voluntary undertaking from the organisation or person concerned, when it has

reasonable grounds to believe that the PDPA has been contravened (Section 48L of the PDPA).

Directions

The PDPC has the power to issue directions to secure compliance with the PDPA (Section 48I of the PDPA). It may give directions to the organisation to ensure compliance, including directions to:

- stop the collection, use or disclosure of personal data in breach of the PDPA;
- destroy personal data collected in breach of the PDPA; or
- provide access or correct the personal data.

Written notice to pay financial penalties

The PDPC may require an organisation to pay 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 any intentional or negligent contravention of the Data Protection Provisions (Section 48J(3) of the PDPA).

14. Are there any expected changes to the online safety landscape in your jurisdiction in 2024–2025?

IMDA will be publishing Annual Online Safety Reports submitted by Designated SMSs to help users make informed choices on services that provide a safe online experience. The first set of Annual Online Safety Reports will be submitted in the second half of 2024 and published on IMDA's website. IMDA will be responding to the Annual Online Safety Reports and make an overall assessment of the SMSs' efforts to enhance online safety.

15. Does your jurisdiction impose 'data protection by design' or 'data protection by default' requirements or similar? If so, please describe the requirement(s) and how businesses typically meet such requirement(s).

While the PDPA does not expressly impose requirements on organisations to adopt concepts such as "data protection by design" or "data protection by default", the PDPC has, in its Guide to Developing a Data Protection Management Programme (revised 14 September 2021), stated that businesses can consider adopting a Data Protection by Design ("**DPbD**") approach to compliance.

Under the DPbD approach, organisations consider the protection of personal data from the earliest possible design stage of any project, throughout the project's operational lifecycle. In tandem with this, the PDPC also issued a Guide to Data Protection by Design for ICT Systems (updated 14 September 2021) to assist organisations that wish to apply DPbD principles when designing and building their ICT systems.

16. Are controllers and/or processors of personal data required to maintain any internal records of their data processing activities or establish internal processes or written documentation? If so, please describe how businesses typically meet such requirement(s).

Internal Processes or Written Documentation

As part of the Accountability Obligation, Section 12 of the PDPA requires the development and implementation of policies and practices that are necessary for the organisation to comply with the PDPA. PDPC considers this to include internal data protection policies and processes. Generally, these policies and practices would need to be in writing (see e.g. *Re Cricket Association and others* [2018] SGPDPC 19).

These "internal policies and processes" are intended to ensure that all employees of the organisation are aware of the specific practices they must adhere to when handing personal data. They include, for example, the notifications to be given to individuals when their personal data is collected, how access and correction requests should be handled, how personal data must be kept and secured, how personal data must be disposed of when no longer required by the organisation and password policies.

The specific internal policies and practices which may be required for a particular organisation would depend on factors such as the types and amount of personal data collected by the organisation.

Internal Records of Data Processing Activities

There is no express requirement under the PDPA for organisations to maintain internal records of its data processing activities.

However, PDPC has stated in its Guide to Developing a Data Protection Management Programme that known risks should be managed through a good understanding of the life cycle and flow personal data in your organisation, e.g., through data inventory maps or data

flow diagrams. In this regard, PDPC recommends that the data inventory also include information on the business purposes for collection, use and disclosure of personal data, how and where the data was collected, whether and how consent was obtained, the individuals and third parties who handle the personal data, as well as the classification of the data to manage user access. They should also deal with when and how the organisation should dispose of or anonymise the personal data for long-term archival. in *Eatigo International Pte. Ltd*. [2022] SGPDPC 9, PDPC reiterated that for an organisation to effectively safeguard personal data, it must first know what its personal data assets are and the surest way to ensure such visibility is to maintain a comprehensive personal data asset inventory.

Separately, where an organisation refuses to provide personal data pursuant to an individual's request for access under Section 21 of the PDPA, the organisation must preserve a complete and accurate copy of such data for the prescribed period, i.e., In brief, for a period of at least 30 calendar days after rejecting the access request to allow time for the individual to seek PDPC's review and if the individual submits an application for review to the PDPC, until the review by PDPC is concluded and any right of the individual to apply for reconsideration and appeal is exhausted (Section 22A PDPA read with Regulation 8 PDP Regulations 2021).

Further, Section 50(4) of the PDPA imposes an obligation on organisations to retain records relating to an investigation, for one year or such longer period as directed, after completion of such investigation. In the case of *Re NTUC Income Insurance Co-operative Ltd* [2018] SGPDPC 10, the PDPC stated that all organisations have the duty to preserve evidence and that the PDPC does not look favourably on the destruction or deletion of potentially relevant documents and records, and depending on circumstances, may impose sanctions on the relevant organisation.

17. Do the data protection laws in your jurisdiction require or recommend data retention and/or data disposal policies and procedures? If so, please describe such requirement(s).

The PDPA requires that organisations cease to retain their 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 the purpose for which that personal data was collected is no longer being served by retention of the personal data, and such retention is no longer necessary for legal or business purposes (Section 25 of the PDPA).

While the PDPA does not expressly provide for defined data retention periods, and data disposal policies and procedures, the PDPA requires that organisations develop and implement policies and practices that are necessary for the organisation to meet its obligations under the Act (Section 12 of the PDPA). Accordingly, PDPC's guidelines state that organisations should put in place (among other things) schedules that define the respective retention limitations for data held and controlled by the organisation (e.g. how long to keep records).

With respect to data retention periods, the duration of time whereby an organisation can retain personal data is assessed on a standard of reasonableness, having regard to the purposes for which the personal data was collected and retained, and legal or business purposes for which retention of the personal data is necessary. As such, legal or specific industry-standard requirements for retention may apply.

The PDPC, in considering whether an organisation has ceased to retain personal data, will consider factors such as whether the organisation has any intention to use or access the personal data, how much effort and resources the organisation would need to expend in order to use or access the personal data again, whether any third parties have been given access to the personal data, and whether the organisation has made a reasonable attempt to destroy, dispose of or delete the personal data in a permanent and complete manner (Key Concept Guidelines).

18. Under what circumstances is a controller operating in your jurisdiction required or recommended to consult with the applicable data protection regulator(s)?

There is no mandatory requirement under the PDPA to consult the PDPC.

Unlike in other jurisdictions, organisations in Singapore do not need to submit their binding corporate rules to the PDPC for approval.

19. Do the data protection laws in your jurisdiction require or recommend risk assessments in connection with data processing activities and, if so, under what

circumstances? How are these risk assessments typically carried out?

There is no standalone requirement to conduct a data protection risk assessment under the PDPA. Notwithstanding, there are certain scenarios in the PDPA in which organisations are required to undertake an assessment.

For example, if an organisation seeks to rely on deemed consent by notification under Section 15A of the PDPA, it must first conduct an assessment to determine that the proposed collection, use or disclosure of the personal data is not likely to have an adverse effect on the individual. This assessment must specify all of the following information:

a. the types and volume of personal data to be collected, used or disclosed;
b. the purpose or purposes for which the personal data will be collected, used or disclosed;
c. the method or methods by which the personal data will be collected, used or disclosed;
d. the mode by which the individual will be notified of the organisation's proposed collection, use or disclosure of the individual's personal data;
e. the period within which, and the mode by which, the individual may notify the organisation that the individual does not consent to the organisation's proposed collection, use or disclosure of the individual's personal data;
f. the rationale for the period and mode mentioned in sub-paragraph (e).

Likewise, if an organisation seeks to rely on the legitimate interests exception under Part 3 of the First Schedule to the PDPA, the organisation is required to conduct an assessment to determine whether the collection, use or disclosure of personal data about the individual is in the legitimate interests of the organisation or another person; and whether the legitimate interests of the organisation or other person outweigh any adverse effect on the individual. This assessment must:

a. specify —
    i. the types and volume of personal data to be collected, used or disclosed;
    ii. the purpose or purposes for which the personal data will be collected, used or disclosed; and
    iii. the method or methods by which the personal data will be collected, used or disclosed;
b. identify any residual adverse effect on any individual after implementing any reasonable measures to eliminate the adverse effect, reduce the likelihood that the adverse effect will occur, or mitigate the adverse effect;
c. identify the legitimate interests that justify the collection, use or disclosure by the organisation of personal data about the individual;
d. where the legitimate interests identified under sub-paragraph (c) relate to a person other than the organisation, identify that other person by name or description; and
e. set out the reasons for the organisation's conclusion that the legitimate interests identified under sub-paragraph (c) outweigh any adverse effect on the individual.

Additionally, to assist organisations in complying with the PDPA, the PDPC has issued its Guide to Data Protection Impact Assessments (published 14 September 2021) ("**DPIA Guide**"), which provides guidance to organisations when conducting a DPIA to identify, assess and address personal data protection risks based on the organisation's functions, needs and processes.

20. Do the data protection laws in your jurisdiction require a controller's appointment of a data protection officer, chief information security officer, or other person responsible for data protection, and what are their legal responsibilities?

The appointment of a DPO is mandatory under the PDPA.

Section 11(3) of the PDPA requires an organisation to designate one or more individuals to be responsible for ensuring that the organisation complies with the PDPA (i.e. a DPO).

Some of the main responsibilities of a DPO include:

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

matters, if necessary.

The business contact information of at least one such DPO must be made available to the public, such that the DPO is able to answer questions relating to the collection, use or disclosure of personal data on behalf of the organisation. The business contact information may be made available to the public via BizFile+ for companies that are registered with the Accounting and Corporate Regulatory Authority.

As best practice, the business contact information of the DPO should be readily accessible from Singapore, operational during Singapore business hours and in the case of telephone numbers, be Singapore telephone numbers. This would facilitate the organisation's ability to respond promptly to any complaint or query on its data protection policies and practices.

To be clear, the legal responsibility for complying with the PDPA remains with the organisation and is not transferred to such designated individual(s).

21. Do the data protection laws in your jurisdiction require or recommend employee training related to data protection? If so, please describe such training requirement(s).

Section 12(c) of the PDPA require organisations to communicate to its staff information about the organisations' policies and practices that are necessary for the organisations to meet their obligations under the PDPA. Such communication could be incorporated into organisations' employee training programmes.

Employee training is also an example of an administrative measure which an organisation should implement to fulfil its obligation to make reasonable security arrangements in accordance with the Protection Obligation (Section 24 of the PDPA).

22. Do the data protection laws in your jurisdiction require controllers to provide notice to data subjects of their processing activities? If so, please describe such notice requirement(s) (e.g., posting an online privacy notice).

An organisation is required to develop and implement policies and procedures that are necessary for the organisation to meet its obligations under the PDPA, and a process to receive and respond to complaints, and to make information relating to the foregoing available on request (Section 12 of the PDPA).

A data protection notice is the most common way to make available information about the organisation's policies and procedures.

In practice, a typical data protection notice would usually contain the following information:

a. the type of personal data the organisation collects, uses and discloses;
b. the purposes for which the organisation collects, uses and discloses personal data;
c. details on how the organisation processes personal data (including transfers to third parties or data intermediaries (if any);
d. details on how the organisation will keep the personal data accurate and up-to-date;
e. the duration of time for which the organisation will keep the personal data;
f. procedures for individuals to make access and correction requests;
g. procedures for individuals to withdraw their consent;
h. details regarding the transfer of personal data to an entity located in another country and the safeguards taken to protect the transferred personal data; and
i. business contact information of the DPO and any complaint/feedback channels.

Additionally, under the Notification Obligation, organisations are required to inform individuals of the purposes for the collection, use or disclosure of personal data, prior to such collection, use or disclosure of such personal data. Generally, organisations also notify individuals of the purposes for which it collects, uses and discloses personal data through their data protection notices.

23. Do the data protection laws in your jurisdiction draw any distinction between the controllers and the processors of personal data, and, if so, what are they?

There is no definition of "data controller" or "data processor" under the PDPA. However, an equivalent concept is that of the organisation and data intermediary (as defined in Question 4).

The data intermediary that processes personal data on behalf of and for the purposes of an organisation pursuant to a written contract, shall only be subject to the Protection Obligation, Retention Limitation Obligation and the obligation to inform the organisation it is

processing data on behalf of, of the occurrence of a data breach (Section 4(2) of the PDPA).

"Processing" is defined in the PDPA to include the "*carrying out of any operation or set of operations in relation to the personal data, such as recording; holding; organisation, adaptation or alteration; retrieval; combination; transmission; erasure or destruction.*"

Section 4(3) of the PDPA provides that an organisation shall have the same obligation under the PDPA in respect of personal data processed by its data intermediary as if the personal data were processed by the organisation itself.

In this connection, 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. The PDPC's Key Concepts Guidelines additionally state that it is important that an organisation is clear as to its rights and obligations when dealing with its vendor and, where appropriate, include provisions in their written contracts that clearly set out each party's responsibilities and liabilities in relation to the personal data in question, including whether one party is to process personal data on behalf of and for the purposes of the other organisation. Without clarity, the risks of omissions will likely fall on the organisation. If there is no contract evidenced or made in writing with the 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 organisation.

24. Do the data protection laws in your jurisdiction place obligations on processors by operation of law? Do the data protection laws in your jurisdiction require minimum contract terms with processors of personal data?

As stated in Question 23 above, a data intermediary that processes personal data on behalf of and for the purposes of an organisation pursuant to a written contract, is subject to the Protection Obligation, Retention Limitation Obligation and the obligation to inform the organisation it is processing data on behalf of, of the occurrence of a data breach (Section 4(2) of the PDPA).

The PDPA does not expressly require organisations engaging data intermediaries to include certain contract terms. Nonetheless, the PDPC, in its Key Concepts Guidelines, advises organisations to undertake an appropriate level of due diligence to assure itself that a potential data intermediary is capable of complying with the PDPA. Furthermore, the PDPC's Guide to Managing Data Intermediaries recommends various measures for managing data intermediaries, as well as terms that should be included in the contract. In particular, the organisation should make clear in its contract the scope of work that the data intermediary is to perform on its behalf and for its purposes (among other things).

The PDPC has also issued a non-binding Guide on Data Protection Clauses for Agreements Relating to the Processing of Personal Data (revised 1 February 2021), which provides some sample clauses that organisations can refer to.

25. Are there any other restrictions relating to the appointment of processors (e.g., due diligence, privacy and security assessments)?

In its Key Concept Guidelines, the PDPC has also clarified that the organisation engaging the data intermediary remains liable to comply with the Transfer Limitation Obligation with respect to any transfers of personal data out of Singapore, e.g. if the personal data is transferred by the organisation to an overseas data intermediary, or transferred overseas by the data intermediary in Singapore as part of its processing on behalf and for the purposes of the organisation. The onus is on the transferring organisation to undertake appropriate due diligence and obtain assurances when engaging a data intermediary.

More generally, the PDPC has stated in its Guide to Managing Data Intermediaries that organisations should ensure that their data intermediaries are able to meet their data processing requirements and provide the protection and care that is commensurate with the volume and sensitivity of the personal data that the data intermediary is processing. Organisations should exercise due diligence in evaluating that their data intermediaries have the necessary data protection framework to ensure that the personal data they process will be properly safeguarded.

26. Please describe any restrictions on monitoring, automated decision-making or profiling in your jurisdiction, including through the use of tracking technologies

such as cookies. How are these terms defined, and what restrictions on their use are imposed, if any?

Monitoring and Profiling

The PDPA does not place any direct restrictions on monitoring or profiling *per se* (including through the use of tracking technologies such as cookies).

Nonetheless, the PDPC has provided guidance on the usage of cookies, which are defined in the Selected Topics Guidelines as "*text files created on a client computer when its web browser loads a website or web application*".

According to the Selected Topic Guidelines, if the data collected from monitoring or profiling activities constitutes personal data, the organisation would be required to comply with the PDPA, such as the Consent Obligation.

In addition, the Purpose Limitation Obligation limits any collection, use or disclosure of personal data about an individual for purposes that, inter alia, a reasonable person would consider appropriate in the circumstances. Therefore, should there be any personal data collected through monitoring or profiling activities carried out by an organisation, this would require the organisation to ensure that the purposes for which any collection, use and/or disclosure is done, are what a reasonable person would consider appropriate in the circumstances.

Ultimately, it depends on whether the cookies in question contain personal data. The PDPA will not apply if the cookies in question do not store or collect personal data. For example, if the session cookie only collects and stores technical data needed to play back a video on a website, consent would not be needed.

Automated Decision-making

The PDPA does not provide individuals with a right not to be subject to a decision based solely on automated decision-making.

27. Please describe any restrictions on targeted advertising and/or cross-contextual behavioral advertising. How are these terms or any similar terms defined?

The PDPA does not define or use the terms "targeted advertising" and "cross-contextual behavioural advertising". However, insofar as targeted and cross-contextual behavioural advertising involves the collection or use of personal data, the individual's express, opt-in consent under the PDPA should be obtained. PDPC also recommends that organisations provide individuals with the ability to set their cookie preferences within the website to enable or disable the use of such cookies for personalised advertisement targeting.

28. Please describe any data protection laws in your jurisdiction addressing the sale of personal data. How is the term "sale" or such related terms defined, and what restrictions are imposed, if any?

There are no laws in place that directly address the sale of personal data.

Nevertheless, the sale or purchase of personal data are activities that fall under the scope of the PDPA. The sale of personal data constitutes disclosure and purchase of personal data constitutes collection. As such, organisations engaging in the sale of personal data have a duty to comply with the data protection obligations under the PDPA, specifically the Consent and Notification Obligations (*Re Amicus Solutions Pte. Ltd.* [2019] SGPDPC 33). Individuals whose personal data is sold must be notified of, and consent to, the sale of their personal data before such data is collected, used or disclosed.

29. Please describe any data protection laws in your jurisdiction addressing telephone calls, text messaging, email communication, or direct marketing. How are these terms defined, and what restrictions are imposed, if any?

Direct marketing is regulated under (a) the Spam Control Act 2007 (2020 Revised Edition) ("**Spam Control Act**"), and (b) the DNC Provisions.

The Spam Control Act provides for the control of spam, i.e., unsolicited commercial communications sent in bulk by electronic mail or by text or multi-media messaging to mobile telephone numbers or instant messaging accounts.

The Spam Control Act defines an "electronic address" as email addresses, instant messaging accounts, as well as mobile telephone numbers to which an electronic message can be sent, and an "electronic message" is defined as a message sent to an electronic address, whether or not the electronic address exists or whether the message reaches its intended destination. However,

an “electronic message” does not include a voice call made using a telephone service.

Under the Spam Control Act, no person shall send, cause to be sent, or authorise the sending of, an electronic message to electronic addresses generated or obtained through the use of (a) a dictionary attack; or (b) an address harvesting software. Additionally, any person sending unsolicited commercial electronic messages in bulk must comply with the requirements in the Second Schedule of the Spam Control Act, including:

a. information on the sender;
b. a clear and conspicuous statement in English setting out the procedure to submit an unsubscribe request;
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.

On the other hand, the DNC Provisions regulate, inter alia, marketing messages and calls (i.e., “specified messages” as defined under Section 37 of the PDPA) to Singapore telephone numbers. Under the DNC Provisions, no person shall send a specified message addressed to a Singapore telephone number unless the sender:

a. prior to the sending of the specified message, either:
    i. verifies against the relevant DNC register to confirm that the telephone number is not listed before sending the message or calling;
    ii. obtains from a checker information that the telephone number is not listed in the relevant DNC register (i.e., the “relevant information”) and has no reason to believe that, and is not reckless as to whether —
        i. the prescribed period in relation to the relevant information has expired; or
        ii. the relevant information is false or inaccurate; or
    iii. obtains clear and unambiguous consent to the sending of the specified message to that number is obtained in evidential form;
b. includes information identifying the sender and details on how the sender can be readily contacted, and that 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, does not conceal or withhold the calling line identity from the recipient.

The DNC Provisions also provide that no person shall send, cause to be sent, or authorise the sending of, messages to Singapore telephone numbers generated or obtained through the use of (a) a dictionary attack; or (b) an address harvesting software.

30. Please describe any data protection laws in your jurisdiction addressing biometrics, such as facial recognition. How are such terms defined, and what restrictions are imposed, if any?

There are no laws that specifically address biometrics, such as facial recognition technology.

Depending on the biometric data involved, such data may fall within the definition of “personal data” under the PDPA. If so, the organisation employing the biometrics solution would be subject to the data protection obligations, such as the Consent Obligation, under the PDPA. PDPC has also issued a Guide on the Responsible Use of Biometric Data in Security Applications to help organisations (e.g., Management Corporation Strata Titles, building or premise owners and security services companies) to use security cameras and biometric recognition systems responsibly and safeguard individuals’ biometric data where it is collected, used or disclosed.

31. Please describe any data protection laws in your jurisdiction addressing artificial intelligence or machine learning (“AI”).

The PDPA governs any processing of personal data, whether in the development or deployment of AI, although it does not have specific obligations addressing AI.

In 21 January 2020, the IMDA and PDPC published the voluntary Model Artificial Intelligence Governance Framework (Second Edition) (“Model Framework”). The Model Framework states that decisions made by AI

should be explainable, transparent and fair, and that AI solutions should be human-centric.

In relation to personal data, the PDPC has published its Advisory guidelines on Use of Personal Data in AI Recommendation and Decision Systems ("**AI Guidelines**") on 1 March 2024. The AI 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.

32. Is the transfer of personal data outside your jurisdiction restricted? If so, please describe these restrictions and how businesses typically comply with them (e.g., does a cross-border transfer of personal data require a specified mechanism or notification to or authorization from a regulator?)

The transfer of personal data outside of Singapore is subject to organisations meeting the requirements under the Transfer Limitation Obligation.

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 and the PDP Regulations, to ensure that the recipients of the personal data provide a standard of protection to the transferred personal data that is comparable to the PDPA.

Under Part 3 of the PDP Regulations, the transferring organisation must, prior to the transfer of personal data outside of Singapore, take appropriate steps to ascertain whether, and ensure that, the recipient of the personal data in that country or territory outside Singapore is bound by legally enforceable obligations to provide to the transferred personal data a standard of protection that is at least comparable to the protection afforded under the PDPA.

In Part 3 of the PDP Regulations, legally enforceable obligations include obligations imposed on a data recipient under:

a. any law;
b. any contract which (i) requires the recipient to provide a standard of protection to the transferred personal data that is at least comparable to the PDPA, and (ii) specifies the countries and territories to which the personal data may be transferred under the contract; and
c. any binding corporate rules that may only be used for recipients that (i) are related to the transferring organisation, (ii) requires every recipient of the transferred personal data that is related to the transferring organisation and does not already have another legally enforceable obligation, to provide a standard of protection for the personal data transferred to the recipient that is at least comparable to the protection under the PDPA, and (iii) must specify the recipients of the transferred personal data to which the binding corporate rules apply, the countries and territories to which the personal data may be transferred under the binding corporate rules, and the rights and obligations provided by the binding corporate rules.

Under the PDP Regulations, a recipient of personal data is related to the transferring organisation transferring that data 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.

Alternatively, a recipient is taken to have satisfied the requirements under the Transfer Limitation Obligation if (a) it is receiving the personal data as an organisation and it holds a valid Asia Pacific Economic Cooperation Cross Border Privacy Rules ("**APEC CBPR**") certification; or (b) it is receiving the personal data as a data intermediary and it holds either a valid APEC CBPR or Asia Pacific Economic Cooperation Privacy Recognition for Processors ("**APEC PRP**") certification, or both.

33. What security obligations are imposed on data controllers and processors, if any, in your jurisdiction?

The Protection Obligation under Section 24 of the PDPA requires each organisation to protect personal data in its possession or under its control by making reasonable security arrangements to prevent (a) unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks; and (b) the loss of any storage medium or device on which personal data is stored.

No specific security arrangements are prescribed, given that there is no one-size-fits-all solution. To this end, the PDPC has recommended, in its Key Concepts Guidelines, that each organisation should:

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

34. Do the data protection laws in your jurisdiction address security breaches and, if so, how do such laws define a "security breach"?

Yes, there is a mandatory data breach notification regime under Part 6A of the PDPA. Under the Data Breach Notification Obligation (Sections 26A to 26E of the PDPA), in the event of a data breach, an organisation is required to conduct an assessment if the data breach is a notifiable data breach, i.e., whether the data breach would (a) result in, or likely result in, significant harm to an affected individual; or (b) is, or is likely to be, of a significant scale. If so, the organisation must notify PDPC within 3 calendar days after the organisation makes that assessment, as well as notify affected individuals in any manner that is reasonable in the circumstances, unless an exception applies. See Question 31 below.

A "data breach" is defined in the PDPA as, in relation to personal data, (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.

Under the Cybersecurity Act, a CII owner must notify the Commissioner of the occurrence of: (a) a prescribed cybersecurity incident in respect of the CII; (b) a prescribed cybersecurity incident in respect of any computer or computer system under the owner's control that is interconnected with or that communicates with the CII; (c)any other type of cybersecurity incident in respect of the CII that the Commissioner has specified by written direction to the owner, within 2 hours of becoming aware of the occurrence (Section 14 of the Cybersecurity Act; Regulation 5(1) of the Cybersecurity (Critical Information Infrastructure) Regulations 2018 ("**CII Regulations**")).

A "prescribed cybersecurity incident" refers to either of the following: (a) any unauthorised hacking of the critical information infrastructure or the interconnected computer or computer system to gain unauthorised access to or control of the CII or interconnected computer or computer system; (b) any installation or execution of unauthorised software, or computer code, of a malicious nature on the CII or the interconnected computer or computer system; (c) any man-in-the-middle attack, session hijack or other unauthorised interception by means of a computer or computer system of communication between the CII or the interconnected computer or computer system, and an authorised user of the CII or the interconnected computer or computer system; (d) any denial of service attack or other unauthorised act or acts carried out through a computer or computer system that adversely affects the availability or operability of CII or the interconnected computer or computer system (Regulation 5(3) of the CII Regulations).

35. Does your jurisdiction impose specific security requirements on certain sectors, industries or technologies (e.g., telecom, infrastructure, AI)?

In the banking and finance sector, the MAS administers the Banking Act, which contains provisions preventing the disclosure of customer information by a bank or the bank's officers. The MAS is empowered under the Monetary Authority of Singapore Act 1970 (2020 Revised Edition) to issue directives and notices that contain requirements relating to data protection and cybersecurity to relevant financial institutions.

Most notably, the MAS has issued Notices and Guidelines on Technology Risk Management, which requires financial institutions to, among others, implement IT controls to protect customer information from unauthorised access or disclosure. This was last updated in January 2021. The MAS has also issued Notices on Cyber Hygiene and Guidelines on Outsourcing. Furthermore, in light of the recent spate of SMS-phishing scams targeting bank customers, MAS and the Association of Banks in Singapore ("**ABS**") introduced a set of additional measures to bolster the security of digital banking, including the requirement to remove clickable links in emails or SMSes sent to retail customers.

In the telecommunications sector, the IMDA prescribes specific rules including provisions in the TCC which pertain to the safeguarding of End User Service

Information, including, among others, information about an end user's usage patterns, as well as the services used by an end user.

Separately, IMDA has established the Telecom Cybersecurity Strategic Committee, as part of its new multi-year roadmap to improve Singapore's telecom cybersecurity capabilities.

The IMDA has also published the Internet of Things ("**IoT**") Cyber Security Guide (published March 2020), which is an informative, voluntary document that provides baseline security recommendations and checklists for the acquisition, development, operations and maintenance of IoT systems. This is targeted at IoT developers, providers and users.

In the healthcare sector, the Health Sciences Authority has published the voluntary Regulatory Guidelines for Software Medical Devices – A Life Cycle Approach (published April 2022) for stakeholders involved in software medical device development and/or supply in Singapore, requiring them to make cybersecurity considerations amongst others.

MOH also issued its Cybersecurity Advisory 1/2019, which advises all licensees to adopt cybersecurity best practices and to implement relevant measures, where appropriate. Additionally, in 2021, MOH issued several advisories in which licensees are encouraged to implement various cybersecurity measures in response to cybersecurity attacks and vulnerabilities.

The PDPC has also published a Guide to Data Protection Practices for ICT Systems, which recommends basic and enhanced practices that organisations should adopt where appropriate for their circumstances.

The CSA has published the Cybersecurity Code of Practice for Critical Information Infrastructure (Second Edition) (revised 12 December 2022) which sets out the minimum protection requirements that CII owners must implement.

36. Under what circumstances must a business report security breaches to regulators, impacted individuals, law enforcement, or other persons or entities? If breach notification is not required by law, is it recommended by the applicable regulator in your jurisdiction, and what is customary in this regard in your jurisdiction?

There is a mandatory data breach notification regime under Part 6A of the PDPA (i.e., Sections 26A to 26E of the PDPA). Under this Data Breach Notification Obligation, an organisation must conduct an assessment of a data breach, in a reasonable and expeditious manner, to determine if the data breach is a "notifiable data breach" (Section 26C of the PDPA).

A notifiable data breach is defined as a data breach that (a) results in, or is likely to result in, significant harm to any individual to whom any personal data affected by a data breach relates; or (b) is, or is likely to be, of a significant scale (i.e. 500 or more individuals).

Upon assessing that the data breach is a "notifiable data breach", the organisation must notify the PDPC soon as practicable, but no later than 3 calendar days, after it makes the assessment (Section 26D of the PDPA). This notification to the PDPC must contain all the relevant information of the data breach to the best of the knowledge and belief of the organisation.

According to the Personal Data Protection (Notification of Data Breaches) Regulations 2021, a data breach is deemed to result in significant harm to an individual if the data breach relates to:

a. the individual's full name or alias or identification number, and any of the personal data or classes of personal data relating to the individual set out in Part 1 of the Schedule, subject to Part 2 of the Schedule; or
b. all of the following personal data relating to an individual's account with an organisation:
    i. the individual's account identifier, such as an account name or number;
    ii. any password, security code, access code, response to a security question, biometric data or other data that is used or required to allow access to or use of the individual's account.

The categories under Part 1 of the Schedule to the Personal Data Protection (Notification of Data Breaches) Regulations 2021 broadly include personal data in the following categories (non-exhaustive list):

- financial information which is not publicly disclosed;
- 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),
- life, accident and health insurance information which is not publicly disclosed;
- specified medical information, including the

assessment and diagnosis of HIV infections;
- information related to adoption matters; or
- a private key used to authenticate any or digitally sign an electronic record or transaction.

Upon notifying the PDPC, the organisation must also notify each individual affected by the data breach in a reasonable manner, unless an exception applies. An organisation does not need to notify affected individuals in two circumstances:

a. if, on or after assessing that the data breach is a "notifiable data breach", the organisation takes any action that renders it unlikely that the data breach will result in significant harm to the affected individual; or
b. if the organisation had implemented, prior to the occurrence of the data breach, any technological measure that renders it unlikely that the data breach will result in significant harm to the affected individual.

One notable exception to the duty to notify is where a data breach takes place within an organisation. A data breach that relates to the unauthorised access, collection, use, disclosure, copying or modification of personal data only within an organisation is deemed not to be a notifiable data breach (Section 26B(4) of the PDPA).

When 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 is required to, without undue delay, notify the other organisation of the occurrence of the data breach. As a good practice, organisations should establish clear procedures for complying with the Data Breach Notification Obligation when entering into contractual arrangements with their data intermediaries.

Apart from the requirements under the PDPA, organisations may also be subject to reporting requirements under sectoral laws and regulations, and would need to report data breaches or other cybersecurity incidents fulfilling certain threshold requirements to regulators such as CSA or MAS.

Under the Cybersecurity Act, a CII owner must notify the Commissioner of the occurrence of: (a) a prescribed cybersecurity incident in respect of the CII; (b) a prescribed cybersecurity incident in respect of any computer or computer system under the owner's control that is interconnected with or that communicates with the CII; (c)any other type of cybersecurity incident in respect of the CII that the Commissioner has specified by written direction to the owner, within 2 hours of becoming aware of the occurrence (Section 14 of the Cybersecurity Act; Regulation 5(1) of the CII Regulations). Please see our response at Question 34.

37. Does your jurisdiction have any specific legal requirements or guidance for dealing with cybercrime, such as in the context of ransom payments following a ransomware attack?

Cyber-crimes are offences under the Computer Misuse Act 1993 (2020 Revised Edition) ("**Computer Misuse Act**"). For example, Section 5 of the Computer Misuse Act criminalises the act of any unauthorised modification to computer material. As ransomware would likely be classified as an "unauthorised modification" to computer material, a person who intentionally conducts ransomware attacks may be found criminally liable under this section.

Under the Cybersecurity Act, the owner of a computer system designated as a CII has to, amongst others, report cybersecurity incidents, and conduct cybersecurity audits and risk assessments in respect of that CII..

The Singapore Computer Emergency Response Team ("**SingCERT**"), which operates under the Cyber Security Agency of Singapore, also provides guidance on cyber security issues, including ransomware attacks. In the event of a cyber security incident, an organisation may choose to inform SingCERT of the incident, and SingCERT may provide technical assistance, and facilitate communications, in response to the incident.

38. Does your jurisdiction have a separate cybersecurity regulator? If so, please provide details.

Yes, the Commissioner of Cybersecurity, appointed under the Cybersecurity Act, is designated as the cybersecurity regulator in Singapore.

Under the Cybersecurity Act, the Commissioner of Cybersecurity has the power to designate a computer or computer system as a CII, if he is satisfied that:

a. the computer or computer system is necessary for the continuous delivery of an essential service, and the loss or compromise of the computer or computer system will have a debilitating effect on the availability of the essential service in Singapore; and

b. the computer or computer system is located wholly or partly in Singapore.

An owner of a CII will be subject to several obligations under the Cybersecurity Act, including but not limited to:

a. furnishing information relating to the CII to the Commissioner of Cybersecurity upon notice given to the owner of the CII;
b. complying with codes of practice and standards of performance issued by the Commissioner of Cybersecurity;
c. abiding by written directions issued by the Commissioner of Cybersecurity;
d. reporting a change in ownership of the CII;
e. reporting a cybersecurity incident in respect of the CII; and
f. conducting regular cybersecurity audits and risk assessments of the CII.

The focus of the Cybersecurity Act is not on securing personal data, but rather to protect CIIs from cybersecurity threats.

39. Do the data protection laws in your jurisdiction provide individual data privacy rights, such as the right to access and the right to deletion? If so, please provide a general description of such rights, how they are exercised, any exceptions and any other relevant details.

The PDPA does not create privacy rights; rather, it imposes obligations on organisations to safeguard the personal data of individuals. Nonetheless, some "rights" that individuals have include the right to withdraw consent, the right to request access to their personal data, and the right to request a correction to their personal data.

Withdrawal of consent: Individuals are allowed to withdraw consent upon giving reasonable notice, and the organisation is required to cease collecting, using or disclosing the personal data, subject to certain exceptions (Section 16 of the PDPA).

Access and correction requests: Pursuant to the Access and Correction Obligations under the PDPA, individuals may request an organisation for access to their personal data, or to correct an error or omission in their personal data, subject to certain exceptions. The individual may also make an application to the PDPC for a review of an organisation's refusal to provide access to their personal data.

To be clear, an individual's right to make an access or correction request is not an unfettered one. The Access Obligation is subject to exceptions in Section 21 and the Fifth Schedule, while the Correction Obligation is subject to the exceptions in Section 22 and the Sixth Schedule. For example, one exception to providing an individual with access to his personal data is where the personal data, if disclosed, would reveal confidential commercial information that could, in the opinion of a reasonable person, harm the competitive position of the organisation (Paragraph 1(g) of the Fifth Schedule).

While there is no right to deletion of personal data, organisations are subject to the Retention Limitation Obligation under the PDPA.

Apart from the PDPA, there exists a framework of common law and statutory torts that collectively protect an individual's privacy, and individuals may be able to pursue their claims for invasions into their privacy under these torts.

40. Are individual data privacy rights exercisable through the judicial system, enforced by a regulator, or both?

As mentioned above, the PDPC is the body in charge of administering and enforcing the PDPA. Members of the public may make a complaint to the PDPC about organisations acting in contravention of the PDPA, albeit the PDPC has discretion in investigating and enforcing the Data Protection Provisions. The individual may also pursue a right of private action through the judicial system for a contravention of the data protection obligations by the organisation (see Question 41 below).

Other statutory torts and common law torts (as discussed at Question 39 above) are exercisable through the judicial system.

41. Do the data protection laws in your jurisdiction provide for a private right of action and, if so, under what circumstances?

Yes, the PDPA provides for a right of private action for individuals. Under Section 48O of the PDPA, any person who suffers loss or damage directly as a result of a contravention of any provision in Parts 4, 5 or 6, 6A or 6B (Part 6B – which relates to data portability – is not yet in force) by an organisation shall have a right of action for relief in civil proceedings in a court, and the court may grant to the applicant relief by way of (a) injunction or declaration; (b) damages; and/or (c) such other relief

as the court thinks fit.

However, if the PDPC has made a decision under the PDPA in respect of a contravention, a private action cannot be brought in respect of that contravention, until the PDPC's decision has become final as a result of there being no further right of appeal.

42. Are individuals entitled to monetary damages or compensation if they are affected by breaches of data protection law? Does the law require actual damage to have been sustained, or is injury to feelings, emotional distress or similar sufficient for such purposes?

Yes, individuals may be entitled to, amongst others, monetary damages or compensation if they are affected by a breach of the PDPA. A civil proceeding brought under Section 48O of the PDPA requires the claimant to show that he has suffered loss or damage directly as a result of a contravention of any provision in Parts 4, 5, 6, 6A or 6B of the PDPA.

In the Court of Appeal decision of *Reed, Michael v Bellingham, Alex (Attorney-General, intervener)* [2022] SGCA 60, it was held that "loss or damage" for an actionable claim under the previous Section 32 (now Section 48O) of the PDPA includes emotional distress but does not include loss of control over personal data. However, in this specific case, the Court of Appeal upheld the District Judge's grant of an injunction and undertaking order, while noting that monetary damages would have been inadequate in light of the risk of further misuse of the Personal Data and the concomitant need to prevent additional emotional distress.

43. How are data protection laws in your jurisdiction enforced?

The PDPC is in charge of enforcing the PDPA. In its Guide to Active Enforcement (revised on 1 October 2022), the PDPC sets out the approach it takes in enforcing the provisions under the PDPA.

When considering whether to take enforcement action, the PDPC is guided by the three key objectives:

a. to respond effectively to breaches of the PDPA where the focus is on those that adversely affect large groups of individuals and where the data involved are likely to cause harm or loss to the affected individuals;
b. to be proportionate and consistent in the application of enforcement action on organisations that are found in breach of the PDPA; where penalties imposed serve as an effective deterrent to those that risk non-compliance to the PDPA; and
c. to ensure that organisations that are found in breach take proper steps to correct gaps in the protection of personal data.

When a potential personal data incident is surfaced to the PDPC (via complaint, self-notification or otherwise), the PDPC will first consider whether it should open an investigation into the matter. The Commissioner may not conduct an investigation into the matter if he is of the view that:

a. the case is better referred to facilitation and/or mediation for resolution;
b. there does not appear to be a breach of the data protection obligations on the facts of the case; or
c. the organisation allegedly in breach is regulated by a sectoral regulator, and the matter would be best handled by the other regulator.

If the PDPC is of the view, however, that an investigation should be conducted, the PDPC will officially open a detailed investigation into the matter, and the investigation process will include the PDPC:

a. issuing notices to produce documents and information to the relevant organisations;
b. conducting interviews and taking statements from the relevant organisations and individuals; and
c. potentially conducting site visits to glean a full view of the facts.

The organisation allegedly in breach will also be given the opportunity to make representations to the PDPC.

After having considered the facts of the case as well as the representations made, the PDPC will then issue its decision on whether the organisation has breached any of the data protection obligations under the PDPA, as well directions (if appropriate), which may include 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.

The Chief Executive of the CSA administers the Cybersecurity Act as the Commissioner of Cybersecurity. At the time of writing, there are no published enforcement actions that have been taken against owners of CII under the Cybersecurity Act.

44. What is the range of sanctions (including fines and penalties) for violation of data protection laws in your jurisdiction?

At present, organisations found to be in breach of the data protection obligations by the PDPC may be issued a notice to pay a financial penalty of up to 10% of the organisation's annual turnover in Singapore, or S$1 million, whichever is higher.

In practice, financial penalties will depend on the specific Data Protection Obligation that was contravened, as well as the severity of the data breach in question.

One example of an egregious breach of the data protection obligations with numerous aggravating factors at play is the case of *Re Singapore Health Services Pte. Ltd. and another* [2019] SGPDPC 3. In that case, the Commissioner, noting that this was the "*largest data breach suffered by any organisation in Singapore with the number of affected individuals amounting to almost 1.5 million unique individuals*", imposed financial penalties on the organisation and its data intermediary of $250,000 and $750,000 respectively, for their failure to put in place reasonable security measures to protect personal data.

Apart from financial penalties, the PDPC is empowered to issue directions for non-compliance as it thinks fit. These include directions requiring the organisation to: stop collecting, using, or disclosing personal data in contravention of the PDPA; destroy personal data collected in contravention of the PDPA; provide access to or correct personal data (Section 48I of the PDPA).

At the time of writing, there are no published enforcement actions that have been taken against owners of CII under the Cybersecurity Act.

45. Are there any guidelines or rules published regarding the calculation of such fines or thresholds for the imposition of sanctions?

Pursuant to Section 48J(6) of the PDPA, the PDPC must have regard to, and give such weight as it considers appropriate to, all the following factors:

- the nature, gravity and duration of the non-compliance by the organisation;
- the type and nature of the personal data affected by organisation's non-compliance;
- whether the organisation, as a result of the non-compliance, gained any financial benefit or avoided any financial loss;
- whether the organisation took any action to mitigate the effects and consequences of the non-compliance, and the timeliness and effectiveness of that action;
- whether the organisation, despite the non-compliance, implemented adequate and appropriate measures for compliance with the PDPA;
- whether the organisation had previously failed to comply with the PDPA;
- the compliance of the organisation with any previous direction issued by the PDPC;
- whether the financial penalty to be imposed is proportionate and effective, having regard to achieving compliance and deterring non-compliance with the PDPA;
- the likely impact of the imposition of the financial penalty on the organisation, including the organisation's ability to continue its usual activities; or
- any other matter that may be relevant (e.g., voluntary notification of the data breach).

46. Can controllers operating in your jurisdiction appeal to the courts against orders of the regulators?

Yes, there is an appeal system in place for appeals against enforcement decisions of the PDPC, including an appeal to the courts.

Reconsideration

An organisation or an individual aggrieved by a decision or direction may apply to the PDPC for the PDPC to reconsider its decision or direction within 28 days of the issuance of the decision or direction. The PDPC may affirm, revoke or vary the contested decision as it thinks fit, and there shall be no further application for reconsideration.

Appeal to Data Protection Appeal Panel

Any organisation or individual aggrieved by, amongst others, any direction, decision, or any reconsideration may, within 28 days after the issue of the direction concerned, appeal to the Chairman of the Data Protection Appeal Panel. The Chairman of the Data Protection Appeal Panel shall appoint a Data Protection Appeal Committee to hear the appeal.

An Appeal Committee hearing an appeal may confirm, vary or set aside the direction or decision which is the subject of the appeal, and, in particular, may:

a. remit the matter to the PDPC;

b. impose or revoke, or vary the amount of, a financial penalty;
c. give such direction, or take such other step, as the PDPC could itself have given or taken; or
d. make any other direction or decision which the PDPC could itself have made.

If the Appeal Committee confirms the direction or decision which is the subject of the appeal, it may nevertheless set aside any finding of fact on which the direction or decision was based.

Appeal to High Court and Court of Appeal

An appeal against, or with respect to, a direction or decision of an Appeal Committee shall lie to the High Court: (a) on a point of law arising from a direction or decision of the Appeal Committee; or (b) from any direction of the Appeal Committee as to the amount of a financial penalty.

The appeal to the High Court may be made only at the instance of:

a. the organisation aggrieved by the direction or decision of the Appeal Committee;
b. if the decision relates to a complaint, the complainant; or
c. the PDPC.

The High Court shall hear and determine the appeal, and may (a) confirm, modify or reverse the direction or decision of the Appeal Committee; and (b) make such further or other order on such appeal, whether as to costs or otherwise, as the Court may think fit.

The appeal to the High Court may be further appealed to the Court of Appeal, as if the appeal heard by the High Court was heard in exercise of its original civil jurisdiction.

47. Are there any identifiable trends in enforcement activity in your jurisdiction?

As of 16 April 2024, the PDPC has published a total of 248 grounds of decisions or summaries of grounds of decisions, with a significant majority of these cases relating to breaches of the Protection Obligation under Section 24 of the PDPA. Common types of breaches of the Protection Obligation include lack of data protection policies, poor password policies, poor vendor management, personal data inadvertently made publicly accessible, and lack of multi-factor authentication.

48. Are there any proposals for reforming data protection laws in your jurisdiction currently under review? Please provide an overview of any proposed changes and the legislative status of such proposals.

As stated in Question 2, on 3 April 2024, the first reading of the Amendment Bill took place in Parliament. The Amendment Bill seeks to amend the Cybersecurity Act, including updating existing provisions relating to the cybersecurity of CII owners would be updated and the widening the CSA's oversight to cover STCCs. Additionally, two new classes of regulated entities, ESCI and FDI, will also introduced. Companies that provide foundational digital infrastructure services would also be required to adhere to cybersecurity codes and standards of practice, and be subject to cybersecurity incident reporting requirementss.

Contributors

Lim Chong Kin
Managing Director, Corporate & Finance
chongkin.lim@drewnapier.com

Anastasia Su-Anne Chen
Director, Corporate & Finance
anastasia.chen@drewnapier.com