

Legal 500 Country Comparative Guides 2025

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; 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 ("**PDP Amendment Act**"). This introduced a number of changes to the PDPA, including an expansion of the concept of deemed consent (to include deemed consent by notification and deemed consent by contractual necessity), the introduction of new exceptions to consent (in particular, the 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 PDP

Amendment Act came into effect on 1 February 2021. On 1 October 2022, the PDP 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.

The Cybersecurity Act empowers the Commissioner of Cybersecurity to designate computer systems as CII if they are essential for the continuous delivery of services critical to national interests. The First Schedule to the Cybersecurity Act lists the essential services covered, spanning industries such as energy, information and communications, water, healthcare, banking and finance, emergency services, aviation, land and maritime transport, government services, and media. Sectors where CII are commonly designated include finance, healthcare, and government, where uninterrupted operations are vital.

Under the Cybersecurity Act, the Commissioner may designate a computer or computer system as a CII if it is satisfied that:

- 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
- the computer or computer system is located wholly or partly in Singapore. (However, please see our response to Question 2 on the Cybersecurity Amendment Act.)

CII owners are subject to a range of obligations, including mandatory reporting of cybersecurity incidents (Section 14), regular cybersecurity audits and risk assessments (Section 15), and the provision of detailed information on the design, configuration, and security of their systems upon request (Section 10).

2. Are there any expected changes in the data protection, privacy or cybersecurity landscape in 2025 - 2026 (e.g., new laws or regulations coming into effect, enforcement of such laws and regulations, expected regulations or amendments)?

On 7 May 2024, the Cybersecurity (Amendment) Act 2024 ("**Cybersecurity Amendment Act**") was passed.

Pursuant to the Cybersecurity Amendment Act, existing provisions in the Cybersecurity Act would be updated to take into account new business models and changes in technology. In particular, the definitions of "computer" and computer systems" would be expanded to include "virtual computer" and "virtual computer system" respectively. Further, the Commissioner would be able to designate computer / computer systems located wholly outside Singapore as CII (if its owner is in Singapore,

among other things).

The Cybersecurity Amendment Act would also widen the CSA's oversight to cover the following new categories:

- a. providers of essential services who do not own the CII used for the delivery of the essential services (i.e. providers of essential services who rely on third-party owned CII);
- b. providers of major foundational digital infrastructure ("**FDI**"), namely cloud computing and data centre facility services (the covered services would be specified in the Third Schedule to the Cybersecurity Act), where the loss or impairment of their service would likely lead to disruption or deterioration of the operation of a large number of organisations;
- c. owners of systems of temporary cybersecurity concern ("**STCCs**"). This relates to systems that are at high risk of cyber-attacks for a time-limited period and would have a serious detrimental effect on Singapore's national interests if compromised;
- d. entities of special cybersecurity interest ("**ESCI**"), where the disruption of a sensitive function that they perform, or the disclosure of sensitive information that they hold, will have a significant detrimental effect on Singapore's national interests.

The Cybersecurity Amendment Act will come into operation on a date to be notified.

Separately, under the PDP Amendment Act, a new obligation concerning data portability has been introduced ("**Data Portability Obligation**"). Although the relevant provisions (Part 6B of the PDPA) have already been passed, they will come into force at a later stage, once accompanying regulations are issued. These upcoming regulations are expected to specify key aspects such as the types of data covered by the data portability requirement, and the technical and procedural mechanisms for data transmission. At the time of writing, there is no indication as to when the accompanying regulations may be released.

3. Are there any registration or licensing requirements for entities covered by these data protection and cybersecurity laws, and if so what are the requirements? Are there any exemptions? What are the implications of failing to register / obtain a licence?

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 that provide managed security operations centre monitoring services and penetration testing services must be licensed (Second Schedule to the Cybersecurity Act).

The licensing requirements are set out in Section 26 of the Cybersecurity Act. Applications must be submitted to the licensing officer in the form and manner prescribed by the regulations. In practice, providers of licensable cybersecurity services must apply to the Cybersecurity Services Regulation Office ("CSRO") for a licence. The application must include the applicable fee (S\$1,000 for business entities and S\$500 for individuals). Additionally, the applicant must satisfy the "fit and proper person" criteria to be granted or to retain a licence. Under Section 26(8) of the Cybersecurity Act, the licensing officer may consider these factors when assessing this criterion:

In the case of an individual –

- that the individual has been convicted in Singapore or elsewhere of any offence involving fraud, dishonesty or moral turpitude;
- that the individual has had a judgment entered against the individual in civil proceedings that involves a finding of fraud, dishonesty or breach of fiduciary duty on the part of the individual;
- that the individual is or was suffering from a mental health condition (for example, psychotic disorder, psychosis, schizophrenia, schizoaffective disorder, delusional disorder, bipolar disorder, psychotic depression, or personality disorder, etc.)
- that the individual is an undischarged bankrupt or has entered into a composition with the creditors of the individual; or
- that the individual has had a licence revoked by the licensing officer previously.

In the case of a business entity –

- that the business entity has been convicted in Singapore or elsewhere of any offence involving fraud, dishonesty or moral turpitude;

- that the business entity has had a judgment entered against the business entity in civil proceedings that involves a finding of fraud, dishonesty or breach of fiduciary duty on the part of the business entity;
- that any officer of the business entity is not a fit and proper person to be an officer of a business entity holding the licence;
- that the business entity is in liquidation or is the subject of a winding up order, or there is a receiver appointed in relation to the business entity, or the business entity has entered into a composition or scheme of arrangement with the creditors of the business entity; or
- that the business entity has had a licence revoked by the licensing officer previously.

Any person who provides any licensable cybersecurity service to other persons and fails to obtain a licence is guilty of an offence and shall be liable on conviction to a fine not exceeding S\$50,000 or to imprisonment for a term not exceeding 2 years or to both.

4. How do the data protection laws in your jurisdiction define "personal data," "personal information," "personally identifiable information" or any equivalent term in such legislation (collectively, "personal data")? Do such laws include a specific definition for special category or sensitive personal data? What other key definitions are set forth in the data protection laws in your jurisdiction (e.g., "controller", "processor", "data subject", etc.)?

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 also defines "data intermediary", as "an organisation which processes personal data on behalf of another organisation but does not include an employee of that other organisation". While the PDPA does not define or use the term "controller", the latter organisation (for whom the data intermediary processes personal data) would in effect be the data controller.

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 principles apply to the processing of personal data in your jurisdiction? For example: is it necessary to establish a "legal basis" for processing personal data?; are there specific transparency requirements?; must personal data only be kept for a certain period? Please provide details of such principles.

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 PDP 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 Obligation 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 processing of personal data? 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)?

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 under other 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, consent would 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.

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.

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

7. What special requirements, if any, are required for processing particular categories of personal data (e.g., health data, children's data, special category or sensitive personal data, etc.)? Are there any prohibitions on specific categories of personal data that may be collected, disclosed, or otherwise processed?

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.

Specifically with regard to children's data, the PDPC issued its Advisory Guidelines on the PDPA for Children's Personal Data in the Digital Environment on 28 March 2024, which apply to organisations whose online products or services are likely to be accessed by children (i.e. individuals who are 18 years of age and below). The PDPC has also dealt with the topic of minors' (i.e. individuals below the age of 21) personal data in its Guidelines on the PDPA for Selected Topics (revised 23 May 2024) ("**Selected Topics Guidelines**"). These advisory guidelines set out the PDPC's interpretation of how the PDPA applies in the context of minors' personal data. See Question 10 below for further details on both advisory guidelines.

Sectoral Laws

As mentioned above, sector-specific laws also apply in conjunction with the PDPA. For example, information relating to customers of financial institutions would be governed by financial sector laws (e.g. Banking Act); and health / medical information may fall under the scope of healthcare sector laws (e.g. the Healthcare Services Act 2020, Health Products Act 2007 and the Medicines Act 1975).

In the event of any inconsistency between the PDPA and the provisions of other legislation, such other legislation will prevail to the extent of the inconsistency.

8. Do the data protection laws in your jurisdiction include any derogations, exemptions, 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.

9. Does your jurisdiction require or recommend risk or impact assessments in connection with personal data processing activities and, if so, under what circumstances? How are these

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.

10. Are there any specific codes of practice applicable in your jurisdiction regarding the processing of personal data (e.g., codes of practice for processing children's data or health data)?

The PDPC has released advisory guidelines that set out the PDPC's interpretation of how the obligations under PDPA apply to the processing of personal data in different contexts.

Children's and Minors' Personal Data

The PDPC has published its Advisory Guidelines on the PDPA for Children's Personal Data in the Digital Environment, which apply to organisations whose online products or services are likely to be accessed by children (i.e. individuals who are 18 years of age and below) (e.g. social media services, technology-aided learning, online games and smart toys and devices). Children's personal data are generally regarded as sensitive personal data and must be afforded a higher standard of protection under the PDPA. Notably, the PDPC considers it unreasonable to use a child's personal data or profile to target harmful or inappropriate content at him or her.

The advisory guidelines also state that children between 13 and 17 years of age may provide valid consent when the policies on the collection, use and disclosure of the child's personal data, as well as the withdrawal of consent, are readily understandable to them. This includes ensuring that the child understands the consequences of providing and withdrawing his consent. If an organisation has reason to believe that a child lacks

sufficient understanding of the nature and consequences of giving consent, it should obtain consent from the child's parent or guardian.

The abovementioned guidelines supplement the PDPC's Selected Topics Guidelines, which provide general guidance for data activities in relation to minors. With respect to consent, the Selected Topic Guidelines state 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. However, 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.

Health Data

Regarding the collection, use and disclosure of personal data by healthcare institutions, the PDPC has published its Advisory Guidelines for the Healthcare Sector (updated 20 September 2023) ("**Healthcare Guidelines**"). The Healthcare Guidelines address the application of some data protection provisions of the PDPA in various scenarios in the healthcare sector (e.g. how consent may apply in common healthcare scenarios, how exceptions to consent may apply, how to handle access and correction requests). For completeness, it ought to be noted that sectoral laws that have specific requirements in relation to health data. In particular, the Healthcare Services Act 2020, the Healthcare Services (General) Regulations 2021 as well as the licensing conditions thereunder contain provisions which address the confidentiality and retention of medical records.

11. Are organisations required to maintain any 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] SGPDP 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 handling 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 of 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] SGPDP 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] SGPDP 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.

12. 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).

13. Under what circumstances is it 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.

14. Do the data protection laws in your jurisdiction require the appointment of a data protection officer, chief information security officer, or other person responsible for data protection? If so, 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. Under the PDP Regulations, this requirement is satisfied if the organisation makes available their DPO's contact information in any of the following manners:

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

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).

15. 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) or recommendation(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; Key Concepts Guidelines).

16. 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.

17. Do the data protection laws in your jurisdiction draw any distinction between the responsibility of controllers and the processors of personal data? If so, what are the implications?

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.

18. 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 or any similar terms defined?

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.

19. Please describe any restrictions on targeted advertising and/or behavioral advertising. How are these terms or any similar terms defined?

The PDPA does not define or use the terms "targeted advertising" and "behavioural advertising". However, insofar as targeted and 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.

20. Please describe any data protection laws in your jurisdiction restricting the sale of personal data. How is the term "sale" or such related terms defined?

There are no laws in place that restrict 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] SGPDP 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.

21. Please describe any data protection laws in your jurisdiction restricting telephone calls, text messaging, email communication, or direct marketing. How are these terms defined?

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.

22. Please describe any data protection laws in your jurisdiction addressing biometrics, such as

facial recognition. How are such terms defined?

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.

23. 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.

On 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, the information that PDPC expects to be notified to consumers, and also set out best practices for service providers (e.g. systems integrators) who support organisations implementing bespoke or fully customisable AI systems.

24. 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.

25. What personal data security obligations are imposed by the data protection laws 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.

26. Do the data protection laws in your jurisdiction impose obligations in the context of security breaches which impact personal data? If so, how do such laws define a security breach (or similar term) and under what circumstances must such a breach be reported to regulators, impacted individuals, law enforcement, or other

persons or entities?

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.

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.

27. Do the data protection laws in your jurisdiction establish specific rights for individuals, 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, and any exceptions.

The PDPA imposes obligations on organisations to safeguard the personal data of individuals. 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.

28. 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 480 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.

29. Are individuals entitled to monetary damages or compensation if they are affected by breaches of data protection law? Does the law require actual and material damage to have been sustained, or is non-material 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 480 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 480) 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.

30. How are data protection laws in your jurisdiction typically 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.

31. 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] SGPDP 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 S\$250,000 and S\$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).

32. 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).

33. Are enforcement decisions open to appeal in your jurisdiction? If so, please provide an overview of the appeal options.

Yes, enforcement decisions of the PDPC are open to appeal in Singapore.

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.

34. Are there any identifiable trends or regulatory priorities in enforcement activity in your jurisdiction?

As of June 2025, the PDPC has published a total of 258 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.

35. Do the cybersecurity laws in your jurisdiction require the implementation of specific cybersecurity risk management measures and/or require that organisations take specific actions relating to cybersecurity? If so, please provide details.

Yes, Singapore's cybersecurity framework requires organisations, particularly owners of CII, to implement specific cybersecurity risk management measures. Under the Cybersecurity Act, and pursuant to Section 11(6), CII owners must comply with the Cybersecurity Code of Practice for Critical Information Infrastructure (the "**Cybersecurity Code**"), effective from 4 July 2022.

The Cybersecurity Code sets out minimum protection standards that CII owners must establish to safeguard their infrastructure. These obligations include developing and maintaining a written cybersecurity risk management framework, a cybersecurity incident response plan, and a crisis communication plan. In addition, CII owners are required to prepare a Business Continuity Plan ("**BCP**") and a Disaster Recovery Plan ("**DRP**") to ensure the continued delivery of essential services in the event of disruptions caused by cybersecurity incidents.

The Commissioner is also empowered to issue written directions to ensure the cybersecurity of CIIs (Section 12), and the Cybersecurity Amendment Act will allow such directions to mandate compliance with prescribed technical and cybersecurity standards.

Apart from the above, there are also sector specific requirements that apply to industries such as finance and healthcare (see our response to Question 40 below).

36. Do the cybersecurity laws in your jurisdiction

impose specific requirements regarding supply chain management? If so, please provide details of these requirements.

The CSA has recognised the increasing complexity and risks in digital supply chains. Therefore, in 2022, the CSA launched the Critical Information Infrastructure Supply Chain Management Programme.

This national strategy aims to enhance the cybersecurity resilience of Singapore's CIIs against growing cyber supply chain threats. The programme proposes a multi-pronged approach with five foundational initiatives: a Cyber Supply Chain Assessment Toolkit to inventory and assess vendor risks; a Cyber Contractual Handbook to standardise cybersecurity terms in vendor contracts; a Vendor Certification Programme to incentivise better cybersecurity practices; a Learning Hub to raise awareness and share best practices; and an International Cooperation platform to collaborate globally on cyber supply chain security. The strategy emphasises transparency, standardisation, continuous risk management, and cross-sector collaboration to protect essential services against sophisticated cyber threats.

This programme serves as a policy guide and a set of recommended measures rather than a specific requirement regarding supply chain management.

Further, the Cybersecurity Amendment Act introduces regulatory oversight of CIIs that are outsourced to third parties ("**third-party-owned CIIs**"). Under the new Part 3A, owners of these systems must meet obligations such as furnishing information on the third-party-owned CII (new Section 16E), adhering to codes of practice, standards of performance, and written directions (new Sections 16G and 35A), conducting regular audits and risk assessments (new Section 16J), and participating in cybersecurity exercises (new Section 16L). They must also secure legally binding commitments from third-party service providers to ensure compliance with the Act (new Sections 16E, 16F, 16G, 16H, 16I, and 16J). Reporting obligations under Part 3A are further detailed in our response to Question 42 below.

37. Do the cybersecurity laws in your jurisdiction impose information sharing requirements on organisations?

The Cybersecurity Act authorises the Commissioner of Cybersecurity to require CII owners to provide information relating to the cybersecurity posture of their CIIs. This includes details on the design, configuration, and security

of the systems, as well as operational information. The Cybersecurity (Critical Information Infrastructure) Regulations 2018 ("**CII Regulations**") further specify the types of information that may be requested, such as network diagrams, component details, and the nature of data processed or stored within the CII.

Additionally, the CSA has the authority to investigate cybersecurity threats and incidents to assess their impact, prevent harm, and reduce the risk of future incidents.

CII owners are also required, under the Cybersecurity Code, to implement procedures for sharing information with the Commissioner about cybersecurity threats, vulnerabilities, and the mitigation measures taken. These information-sharing obligations are designed to enable organisations to leverage collective threat intelligence efforts and take proactive steps to prevent or mitigate cyber incidents.

In addition to the Cybersecurity Act, government agencies are working to establish administrative frameworks and partnerships aimed at promoting information sharing. For instance, the MAS partnered with the Financial Services Information Sharing and Analysis Center ("**FS-ISAC**"), an international consortium focused on cyber intelligence for financial institutions, to launch the FS-ISAC Asia Pacific Regional Analysis Centre in Singapore in 2017. This centre is dedicated to facilitating the exchange of threat intelligence and providing actionable insights, tools, and resources to support incident response efforts.

38. Do the cybersecurity laws in your jurisdiction require the appointment of a chief information security officer, regulatory point of contact, or other person responsible for cybersecurity? If so, what are their legal responsibilities?

The Cybersecurity Act does not expressly require the appointment of chief information security officers, regulatory point of contact, or other person responsible for cybersecurity within organisations.

39. Are there specific cybersecurity laws / regulations for different industries (e.g., finance, healthcare, government)? If so, please provide an overview.

Yes, in addition to the Cybersecurity Act, which applies primarily to CIIs across various sectors, there are also sector-specific cybersecurity laws and guidelines that

govern industries such as finance, healthcare, and government.

Financial Services Sector

In the financial services industry, the MAS has outlined risk management principles and best practices in its Guidelines on Technology Risk Management Guidelines. These guidelines are aimed at helping financial institutions: (a) build a strong and resilient technology risk management framework; (b) enhance the security, reliability, resilience, and recoverability of their systems; and (c) implement robust authentication measures to safeguard customer data, transactions, and systems. Key requirements include establishing a technology risk management framework overseen by the board and senior management to identify, assess, monitor, report, and manage technology risks.

Additionally, MAS has issued notices on cyber hygiene, mandating financial institutions to apply security patches to address system vulnerabilities. MAS has also issued its Guidelines on Outsourcing detailing expectations for financial institutions (including banks) that outsource, or intend to outsource, business functions to external service providers.

Healthcare Sector

Following the 2018 SingHealth data breach involving the personal medical information of 1.5 million individuals (*Re Singapore Health Services Pte. Ltd. & Ors.* [2019] SGPDP 3), the MOH released Cybersecurity Advisory 1/2019. In this advisory, healthcare licensees (e.g. hospitals, clinics) are strongly encouraged to review the Committee of Inquiry's findings and adopt recommended cybersecurity best practices as appropriate.

Further, the MOH has also developed the Healthcare Cybersecurity Essentials (MOH Circular No. 105/2021), providing guidance for licensees under the Private Hospitals and Medical Clinics Act 1980 (now repealed) to adopt essential cybersecurity measures to protect IT systems and sensitive data. The Cyber & Data Security Guidelines for Healthcare Providers (MOH Circular No. 85/2023) was also released (which applies to licensees under the Private Hospitals and Medical Clinics Act 1980 and Healthcare Services Act 2020) to provide guidance on the cyber and data security measures for the proper storage, access, use and sharing of health information in order to improve healthcare providers' security postures in the lead up to the implementation of the Health Information Bill.

Telecommunications Sector

In the telecommunications field, the IMDA has issued the Telecommunication Cybersecurity Codes of Practice, which major Internet Service Providers in Singapore must comply with. These Codes cover security incident management and set out requirements to prevent, protect against, detect, and respond to cybersecurity threats, drawing on international standards such as ISO/IEC 27011 and IETF Best Current Practices.

IMDA has also introduced the Singapore SMS Sender ID Registry ("**SSIR**") to combat online scams. From 31 January 2023, all organisations using SMS Sender IDs must register with the SSIR. Unregistered Sender IDs will be blocked, and non-registered SMS IDs will be labelled with the header "Likely-SCAM" during a six-month transition period.

Additionally, as of 31 October 2022, telecom operators must deploy SMS anti-scam filtering solutions within their networks to automatically block potential scam messages before they reach consumers.

40. What impact do international cybersecurity standards have on local laws and regulations?

The Singapore government has indicated that the Cybersecurity Act is guided by internationally recognised standards and seeks to align cybersecurity frameworks and incident-reporting protocols with global practices.

Singapore's approach to cybersecurity is rooted in its commitment to international compliance and collaboration. Since 2021, Singapore has chaired the United Nations Open-Ended Working Group on the Security of and in the Use of Information and Communications Technologies which is the only United Nations ("**UN**") platform dedicated to cybersecurity and promoting responsible state behaviour in cyberspace. Additionally, Singapore actively participates in the UN Group of Governmental Experts, where it has reaffirmed the application of international law, particularly the UN Charter, to cyberspace. This stance is further reinforced by Singapore being a signatory to the Paris Call for Trust and Security in Cyberspace.

Following ASEAN's adoption of the 11 voluntary, non-binding norms for responsible state behaviour in the use of ICTs in 2018, Singapore has collaborated with the UN to drive the regional implementation of these norms. Furthermore, Singapore's regulatory framework is shaped and influenced by international standards and best practices. Both the Telecommunications Cybersecurity Code of Practice and the Singapore Common Criteria Scheme align with international benchmarks, specifically

ISO/IEC 27011 and ISO/IEC 15408, respectively.

41. Do the cybersecurity laws in your jurisdiction impose obligations in the context of cybersecurity incidents? If so, how do such laws define a cybersecurity incident and under what circumstances must a cybersecurity incident be reported to regulators, impacted individuals, law enforcement, or other persons or entities?

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).

A "prescribed cybersecurity incident" refers to either of the following: (a) any unauthorised hacking of the CII 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).

42. How are cybersecurity laws in your jurisdiction typically enforced?

The Commissioner of Cybersecurity, in collaboration with the team at the CSA, oversees the enforcement of the provisions set out in the Cybersecurity Act. At the time of writing, there are no published enforcement actions that have been taken against owners of CII under the Cybersecurity Act.

43. What powers of oversight / inspection / audit do regulators have in your jurisdiction under cybersecurity laws.

Under the Cybersecurity Act, the Commissioner of Cybersecurity is granted authority under Sections 19 and 20 to investigate and respond to cybersecurity incidents. These powers include the ability to issue a written notice requiring any individual to produce physical or electronic records or documents to an incident response officer appointed by the Commissioner.

Additionally, the new Section 29A under the Cybersecurity Amendment Act provides licensing officers, who oversee licensable cybersecurity service providers, with monitoring powers. These powers encompass the authority to enter premises, conduct inspections, and require the production of records, accounts, and documents from licensed providers. Non-compliance with such requirements constitutes a criminal offence.

Under the Cybersecurity Amendment Act, the CSA will also be authorised to inspect the facilities of CII owners if the Commissioner of Cybersecurity has reason to believe that a CII owner has failed to meet its statutory obligations or has provided false, misleading, inaccurate, or incomplete information, as stipulated under the new Section 15(4) of the Cybersecurity Act.

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

There is a range of sanctions for violations of cybersecurity laws in Singapore.

Under the Cybersecurity Act, a CII owner who, without reasonable excuse, fails to report a cybersecurity incident involving a CII commits an offence. Upon conviction, the owner may be subject to a fine of up to S\$100,000, imprisonment for up to two years, or both.

Following the Cybersecurity Amendment Act, stricter penalties will apply to offences involving ECSI and FDI service providers. These offences will carry a fine of up to the greater of S\$200,000 or 10% of the organisation's annual turnover in Singapore. In cases of continuing offences, an additional fine of up to S\$5,000 may be imposed for each day the offence persists after conviction.

The amendments also introduce a new civil penalty framework. Under the new Section 37A of the Cybersecurity Act, the CSA is empowered to impose civil

penalties instead of pursuing prosecution for breaches of any provision under Parts 3, 3A, 3B, 3C, or 3D. The civil penalty may be as high as 10% of the business's annual turnover in Singapore or S\$500,000, whichever amount is greater.

As of the date of this publication, 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?

There are no guidelines or rules published regarding the calculation or such fines or imposition of such sanctions.

46. Are enforcement decisions open to appeal in your jurisdiction? If so, please provide an overview of the appeal options.

For CII owners, the Cybersecurity Act provides mechanisms to appeal to Minister under Section 17. A CII owner who is aggrieved by

- the decision of the Commissioner to issue the notice under Section 7(1) designating the CII as such;
- a written direction of the Commissioner under Sections 12 or 16(2); or
- any provision in any code of practice or standard of performance issued or approved by the Commissioner that applies to the owner, or any amendment made to it may file an appeal to the Minister against the decision, direction, provision or amendment.

Appeals must be filed within 30 days after the date of the notice or direction, or the issue, approval or amendment (as the case may be) of the code of practice or standard of performance, as the case may be, (unless extended by the Minister). The appeal must clearly state the circumstances under which the appeal arises, the issues and grounds for the appeal and submit to the Minister all relevant facts, evidence and arguments for the appeal.

The Minister may confirm, vary, or reverse decisions, or order reconsideration by the Commissioner of any

decision, notice, direction, provision of a code of practice or standard of performance, or an amendment to such code or standard.

Before determining an appeal, the Minister may consult any Appeals Advisory Panel established for the purpose of advising the Minister in respect of the appeal. For technically complex cases, the Minister may also establish an Appeals Advisory Panel under Section 18 of the Cybersecurity Act comprising experts to provide advice to the Minister in respect of the appeal. The Minister is not bound by the advice of the Panel.

Crucially, unless otherwise directed, the original decision remains enforceable during the appeal process, and the Minister's final determination cannot be further appealed.

For Cybersecurity Service Providers, under Section 35 of the Cybersecurity Act, any person whose application for a licence or for the renewal of a licence has been refused by the licensing officer may, within the relevant period after being notified of such refusal, appeal against the refusal in the prescribed manner to the Minister. The "relevant period" is 14 days or such longer period as the Minister allows. The Minister's determination under this section is final.

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

The Cybersecurity Amendment Act, which broadens the scope of regulated entities and strengthen the enforcement powers of the Commissioner of Cybersecurity, reflects Singapore's proactive approach to evolving technological trends and emerging threats. Building on these efforts, it was announced on 1 March 2024 that the Taskforce on the Resilience and Security of Digital Infrastructure and Services is considering the introduction of a Digital Infrastructure Act. Unlike the Cybersecurity Act, which primarily addresses cyber-related risks, the proposed legislation aims to tackle a wider range of resilience challenges faced by digital infrastructure and service providers. These challenges may include not only cybersecurity vulnerabilities, such as misconfigurations in technical architecture, but also physical hazards like fires and failures in cooling systems.

Contributors

Lim Chong Kin

Managing Director, Corporate & Finance

chongkin.lim@drewnapier.com



Anastasia Su-Anne Chen

Director, Corporate & Finance

anastasia.chen@drewnapier.com

