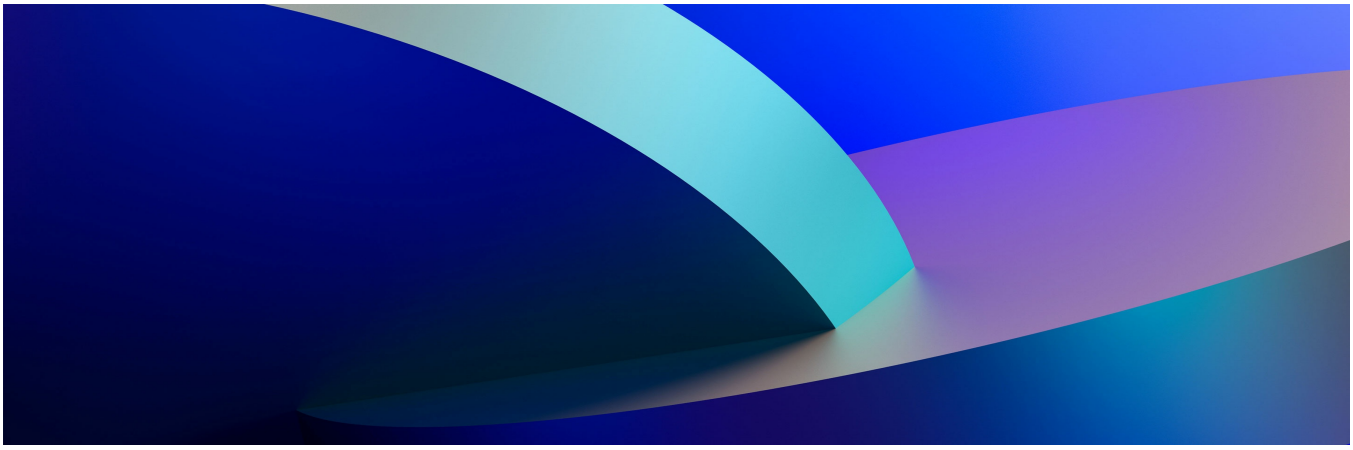

# Data protection and cybersecurity laws in Singapore

## Data protection

### 1. Local data protection laws and scope

The Personal Data Protection Act 2012 (**PDPA**) is the data protection law that governs the collection, use, disclosure and handling of personal data. It recognises both the rights of individuals to protect their personal data, including rights of access and correction, and the needs of organisations to collect, use or disclose personal data for legitimate and reasonable purposes.

The PDPA also provides for the establishment of a national Do Not Call (**DNC**) Registry. The DNC Registry allows individuals to register their Singapore telephone numbers to opt out of receiving marketing phone calls, mobile text messages such as SMS or MMS, and faxes from organisations.

Some key subsidiary legislation that operates alongside the PDPA include the Personal Data Protection Regulations 2021, Personal Data Protection (Notification of Data Breaches) Regulations 2021 and Personal Data Protection (Do Not Call Registry) Regulations 2013.

### 2. Data protection authority

The Personal Data Protection Commission (**PDPC**)

### 3. Anticipated changes to local laws

The following changes to the PDPA have been passed by Singapore's Parliament, however they have not yet come into effect:

- Data portability – mandatory obligation for organisations to provide an individual's data, at the individual's request, to another organisation in a commonly used machine-readable format;
- Provisions which exempt organisations from the proposed data portability obligation and the obligations to provide an individual with access to or to correct personal data at the individual's request in respect of "derived personal data" (i.e. new data that is created through the processing of other data by applying business-specific logic or rules

New Advisory Guidelines 1  which will likely be published in 2024 include the following:

- Advisory Guidelines on Use of Personal Data in AI Recommendation and Decision Systems
- Advisory Guidelines on the Personal Data Protection Act for Children's Personal Data

### 4. Sanctions & non-compliance

**Administrative sanctions:**

- In relation to intentional or negligent contraventions of the PDPA provisions on or after the date of commencement of section 24 of the Personal Data Protection (Amendment) Act 2020 by an organisation whose annual turnover in Singapore exceeds SGD $10 million, a fine not exceeding 10% of the annual turnover in Singapore of the organisation, and in any other case, a fine not exceeding SGD $1 million for each breach.
- In relation to the enforcement of the DNC Registry provisions, the PDPC may issue a fine not exceeding SGD $200,000 in the case of an individual, and in any other case, a fine not exceeding SGD $1 million.
- In relation to the prohibition on use of dictionary attacks and address-harvesting software, the PDPC may issue a fine not exceeding SGD $200,000 in the case of an individual, and in the case of an organisation, in relation to a contravention on or after 1 October 2022 by an organisation whose annual turnover in Singapore exceeds SGD $20 million, a financial penalty not exceeding 5% of the annual turnover of the organisation in Singapore, and in any other case, a financial penalty not exceeding SGD $1 million.
- The PDPC may also issue directions for non-compliance, which includes directions to stop the collection, use or disclosure of personal data, and to destroy any personal data collected.

**Criminal sanctions:**

- Imprisonment for a term not exceeding:
  - Two years – for knowing or reckless unauthorised disclosure of personal data; knowing or reckless unauthorised use of personal data for a gain or to cause a harm or loss to another person; or knowing or reckless unauthorised re-identification of anonymised information;
  - 12 months – for unauthorised requests to access or correct personal data about another individual; intentional disposal, falsification, concealment or destruction of personal data or information about the collection, use or disclosure of personal data by the individual or another individual on behalf of the first mentioned individual; obstructing or hindering the PDPC in the exercise of its powers or duties; knowing or reckless false statement made to the PDPC; or knowing attempts to mislead the PDPC; or
  - Six months – for neglect or refusal to provide any information or produce any document to the PDPC or attend before the PDPC without reasonable excuse; or unauthorised use of a symbol or representation identical to or which resembles that of the PDPC.
- Criminal fines may also be imposed and varies depending on the specific offence, although in general not exceeding SGD $10,000 in the case of individuals who commit a non-continuing offence (with a further maximum fine of SGD $1,000 per day that the offence continues after conviction), and SGD $100,000 in the case of organisations.

**Others**

Individuals have a private right of action and may seek relief by way of injunction, declaration or damages for damages or losses suffered directly as a result of a contravention of the Parts 4, 5, 6, 6A, or 6B of the PDPA by an organisation, or Part 9 (Division 3) or section 48B(1) of the PDPA by an individual.

Where the PDPC has reasonable grounds to believe that an organisation has not complied, is not complying or is likely not to comply with the PDPA provisions or the DNC provisions, the PDPC may exercise its discretion to accept a written voluntary undertaking from the organisation or person concerned instead of carrying out an investigation or issuing directions. Voluntary undertakings may include an undertaking to take specified action within a specified time (for e.g., for the organisation to improve its cyber-defences) or an undertaking to refrain from taking any action (for e.g., for the organisation to stop using personal data collected without consent).

**5. Registration / notification / authorisation**

There is no requirement for organisations to register with the PDPC. However, voluntary registration of the Data Protection Officer is encouraged.

**6. Main obligations and processing requirements**

Organisations, wherever located, that process personal data of individuals in Singapore are required to comply with the PDPA. The PDPA sets out ten main data protection obligations which are to be complied with when processing personal data.

Under the PDPA, to collect and process personal data lawfully, organisations must comply with the following obligations:

- Consent Obligation – to obtain the consent of the individual;
- Purpose Limitation Obligation – to collect, use or disclose personal data about an individual for the purposes that a reasonable person would consider appropriate in the circumstances and for which the individual has given consent;
- Notification Obligation – to notify individuals of the purposes for which the organisation is intending to collect, use or disclose their personal data on or before such collection, use or disclosure of personal data;
- Access and Correction Obligation – upon request, provide information in which the individual's personal data has been or may have been used or disclosed and to correct any error or omission in an individual's personal data;
- Accuracy Obligation – make reasonable effort to ensure that personal data collected by or on behalf of the organisation is accurate and complete, provided that the personal data is likely to be used by the organisation to make a decision that affects the individual or is likely to be disclosed by the organisation to another organisation.
- Protection Obligation – make reasonable security arrangements to protect the personal data that the organisation possesses or controls;
- Retention Limitation Obligation – cease retention of personal data or remove the means by which the personal data can be associated with particular individuals when it is no longer necessary for any business or legal purpose;
- Transfer Limitation Obligation – ensure that the standard of protection provided to the personal data transferred to another country will be comparable to the protection under the PDPA;
- Data Breach Notification Obligation – assess whether a data breach is notifiable and notify the affected individuals and/or PDPC where it is assessed to be notifiable; and
- Accountability Obligation – implement policies and procedures to meet its obligations under the PDPA, and make information about its policies and practices publicly available and to appoint a data protection officer.

Organisations that have contracted to process personal data on behalf of another organisation may be considered a "data intermediary". A data intermediary that processes personal data pursuant to a written contract will only be responsible for the Protection Obligation, the Retention Obligation and the

Data Breach Notification Obligation – protecting the personal data in its care, ensuring that the personal data is not retained by the data intermediary when there is no longer a business or legal need to do so, and notifying the organisation or public agency for which it is processing personal data on behalf of where the data intermediary discovers that a data breach has occurred.

**7. Data subject rights**

Under the PDPA, individuals have the following rights:

- private right of action for direct loss or damage suffered directly as a result of the contravention of the PDPA;
- right to ask the organisation to provide the contact of a person who can answer, on behalf of the organisation, their questions about the collection, use or disclosure of the personal data;
- right to withdraw their consent for the collection, use or disclosure of their personal data by an organisation at any time, with reasonable notice;
- right to request access to their personal data that an organisation possesses or controls, including to be provided with information about the ways in which such personal data has or may have been used or disclosed within the year before the request;
- right to request an organisation to correct an error or omission in their personal data; and
- right to file a complaint.

**8. Processing by third parties**

An organisation must observe the same obligations under the PDPA in respect of personal data processed on its behalf by a data intermediary as if the personal data were processed by the organisation itself.

Data intermediaries that process personal data on behalf of and for the purposes of another organisation pursuant to a written contract will only be subject to the Protection Obligation, the Retention Obligation and the Data Breach Notification Obligation.

**9. Transfers out of country**

There is a limitation on transfers of personal data outside Singapore unless certain conditions are met. The transfers of personal data outside of Singapore requires the recipient of the personal data to provide safeguards equivalent to or greater than the requirements under the PDPA. The PDPA does not provide a white-list of countries that are deemed to have equivalent protection. As such, organisations may transfer personal data overseas if they have taken appropriate steps to comply with the data protection provisions in respect of the transferred personal data while such personal data remains in their possession or control.

When the personal data is transferred to a recipient outside of Singapore, organisations need to ensure that the recipient is bound by legally enforceable obligations to provide a standard of protection comparable to that under the PDPA. Such legally enforceable obligations include obligations imposed under law, any contract, binding corporate rules or any other legally binding instrument. In addition, organisations and data intermediaries that are certified under the Asia-Pacific Economic Cooperation Cross Border Privacy Rules System or Asia-Pacific Economic Cooperation Privacy Recognition for Processors system are deemed to be bound by legally enforceable obligations for the purpose of transfers of personal data outside Singapore.

**10. Data Protection Officer**

Organisations are required to designate at least one individual, known as the Data Protection Officer (DPO), to oversee the data protection responsibilities within the organisation and ensure compliance

with the PDPA. The business contact information of the DPO must be made available to the public. Although not a legal requirement, in practice, the PDPC does request for the information of the DPO to be registered with it.

**11. Security**

Organisations must protect personal data in their possession or under their control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks, and the loss of any storage medium or device on which personal data is stored.

**12. Breach notification**

Organisations are required to assess whether a data breach is notifiable, and to notify the affected individual(s) (where required) and/or the PDPC where the data breach is assessed to be notifiable. A data breach is assessed to be notifiable where:

- the scale of the data breach is of a significant scale, i.e. where it involves the personal data of 500 or more individuals; or
- the data breach is deemed to result in significant harm to affected individual(s) where the compromised personal data relates to:
  - the individual's full name or alias or identification, in combination with:
    - financial information that is not publicly disclosed;
    - identification of vulnerable individuals;
    - life, accident and health insurance information that is not publicly disclosed;
    - specified medical information; or (e) information related to adoption matters; or
    - private key used to authenticate or sign an electronic record or transaction; or
  - individual's account identifier and data for access into the account.

Organisations must notify the PDPC as soon as practicable, but no later than 3 calendar days after it makes the assessment that a data breach is notifiable. The Advisory Guidelines on Key concepts in the PDPA clarifies that the first day starts on the day after the organisation makes the determination that there is a notifiable breach. For example, if the organisation determines on 1 January that a data breach is notifiable, it must notify the PDPC by 4 January. In addition, data intermediaries that process personal data on behalf of and for the purposes of another organisation or a public agency are not required to assess whether the breach is notifiable or to notify the PDPC, but are required to notify that other organisation or public agency when a potential or actual data breach is detected without undue delay.

Sector specific regulation, such as the Notices and Guidelines on Technology Risk Management issued by the Monetary Authority of Singapore, may also require breach notification under different timelines.

**13. Direct marketing**

The DNC provisions of the PDPA generally prohibit organisations from sending marketing messages (in the form of voice calls, text or fax messages) of a commercial nature to Singapore telephone numbers, including mobile, fixed-line, residential and business numbers, registered with the DNC Registry, unless the consumer has provided their clear and unambiguous consent in written or other accessible form for sending the marketing message to the Singapore telephone number.

The organisation may still send a direct marketing message where the sole purpose of the message is:

- to facilitate, complete or confirm an earlier transaction between the sender and recipient;
- to provide warranty information, product recall information, or safety or security information with

respect to a product/service purchased by the recipient;
- to deliver goods or services that the recipient is entitled to receive under an existing transaction; or
- related to the subject matter of an ongoing relationship between the sender and the recipient.

Individuals may subsequently opt out of receiving direct marketing messages. Upon receiving an individual's opt-out request, the organisation must stop sending such messages to that individual's telephone number 21 days after the opt-out.

Under the PDPA, organisations are not permitted to send, cause to be sent or authorise to send any message with a Singapore link to telephone numbers generated or obtained through the use of a dictionary attack or address-harvesting software. This prohibition also applies with respect to electronic messages generated or obtained through the use of a dictionary attack or address-harvesting software under the Spam Control Act 2007.

In addition, under the Spam Control Act 2007, organisations are prohibited to send, cause to be sent or authorise to send any unsolicited commercial electronic messages in bulk if they do not comply with the statutory conditions (e.g. the message needs to include an email address to which the recipient may submit an unsubscribe request).

**14. Cookies and adtech**

The PDPA applies to the collection, use or disclosure of personal data using cookies. However, consent is not required for cookies that:

- do not collect personal data; and
- for internet activities clearly requested by the individual where the individual is aware of the purposes of such collection, use and disclosure and has voluntarily provided his personal data for such purposes.

If the individual configures his browser to accept certain cookies but rejects other, he may be found to have consented to the collection, use and disclosure of his personal data by the cookies he has chosen to accept. In such a circumstance, the PDPC has confirmed that consent can be implied. However, the failure of an individual to actively manage his browser settings does not imply that he has consented to the collection, use and disclosure of his personal data.

**15. Risk scale**

Moderate

**16. Useful links**

Personal Data Protection Act 2012

Personal Data Protection (Notification of Data Breaches) Regulations 2021

Spam Control Act 2007

Advisory Guidelines on Key Concepts in the Personal Data Protection Act

Advisory Guidelines on the Personal Data Protection Act for Selected Topics

## Cybersecurity

**1. Local cybersecurity laws and scope**

The Cybersecurity Act 2018 governs the prevention, management and response to cybersecurity threats and incidents, and regulates owners of critical information infrastructure and cybersecurity service providers. The provisions generally apply to any critical information infrastructure, computer and computer system located wholly or partly in Singapore. The provisions also apply to the Singapore Government, except that the Singapore Government will not be liable to prosecution for an offence.

The related regulations and code of practice that operate alongside the Cybersecurity Act 2018 are the Cybersecurity (Critical Information Infrastructure) Regulations 2018, Cybersecurity (Confidential Treatment of Information) Regulations 2018 and the Cybersecurity Code of Practice for Critical Information Infrastructure.

The Computer Misuse Act 1993 (**CMA**) is the principal legislation on cybercrimes. The CMA applies to any person regardless of nationality and citizenship, outside as well as within Singapore, where the accused, computer program or data was in Singapore at the material time of the offence or the offence causes or creates a significant risk of serious harm in Singapore.

Local cybersecurity laws also include sector-specific rules, such as guidelines and notices issued by the Monetary Authority of Singapore for the financial sector (**MAS Rules**).

**2. Anticipated changes to local laws**

On 15 December 2023, the Cyber Security Agency of Singapore (CSA) announced its intentions to update Singapore’s cybersecurity laws.
The Cybersecurity (Amendment) Act 2024, which was passed but is not yet in force, will update the Cybersecurity Act 2018 by:

- extending the reach of the Cybersecurity Act 2018 to govern Critical Information Infrastructure (CII) located wholly outside Singapore;
- enabling CII providers to leverage new technologies such as cloud services, and requiring them to ensure the security of their outsourced service providers;
  enabling CII providers to leverage new technologies such as cloud services, and requiring them to ensure the security of their outsourced service providers (including mandatory vendor due diligence and reporting);
- creating new frameworks to govern foundational data infrastructure, entities of special cybersecurity interest, and systems of temporary cybersecurity concern;
- requiring entities regulated under the Cybersecurity Act 2018 to adhere to cybersecurity codes of practice and standards of performance and report cybersecurity incidents to the CSA. Such entities must also comply with directions issued by the Commissioner of Cybersecurity to take steps to secure the cybersecurity of specific computer systems under their charge;
- introducing powers for the Commissioner of Cybersecurity to grant time extensions for requirements under the CSA and to authorise an onsite inspection to ascertain compliance.

On 18 April 2023, the Ministry of Home Affairs and the Smart Nation and Digital Government Office announced a set of proposed amendments to the Computer Misuse Act 1993 (CMA), to curb the facilitation of scams and the abuse of Singpass.
The amendments to the CMA came into effect on 8 February 2024, making it an offence for:

- an individual to disclose his own Singpass credentials to facilitate an offence; and
- a person to obtain, retain, supply, offer to supply, transmit or make available, the Singpass credentials of another person to commit or facilitate the commission of any offence.

**3. Application**

- **Cybersecurity Act 2018:** The Cybersecurity Act 2018 requires and authorises the taking of

measures to prevent, manage and respond to cybersecurity threats and incidents; regulates CII owners; establishes the framework for the sharing of cybersecurity information; and regulates cybersecurity service providers. It also provides the regulator with the power to investigate cybersecurity threats or incidents in order to determine their impact, prevent further harm and future incidents. These investigative powers can be delegated to authorised persons, and can be exercised in respect of any computer or computer system in Singapore; not only CIIs. The level of intrusiveness of such powers that can be exercised will depend on the severity of the situation.

- **CMA**: CMA makes provision for securing computer material against unauthorised access or modification, and to require or authorise the taking of measures to ensure cybersecurity. In particular, the CMA criminalises cybercrime such as e-commerce scams and hacking, and also makes it illegal for:
  - any person to provide or receive personal information which he suspects was obtained through unauthorised means; and
  - any person to deal with items designed for, adapted to and used to commit computer crimes, including hardware and software (e.g. computer programmes, passwords or access codes).

- **MAS Rules**: The MAS Rules, amongst other things, require regulated entities to: (a) conduct system and penetration testing; (b) continuously monitor and detect network and other types of cyber intrusions; and (c) require the board and senior management of the regulated entities to effectively implement that entity's cyber resilience programme.

### 4. Authority

The Cyber Security Agency of Singapore

### 5. Key obligations

#### Cybersecurity Act 2018:

- Owners of critical information infrastructure must: (a) comply with codes and directions; (b) conduct audits and risk assessments; (c) report cybersecurity incidents; and (d) participate in cybersecurity exercises; and
- Certain cybersecurity service providers will need to be licensed.

#### CMA:

- The following activities are prohibited: (a) unauthorised access or modification of computer material; (b) unauthorised use or intercept of computer services; (c) obstructing the use of computers; (d) unauthorised disclosure of computer access codes; (e) providing, receiving or supplying personal information which the person knows or suspects was obtained through unauthorised means; and (f) dealing with items designed for, adapted to and used to commit computer crimes.

#### MAS Rules:

- Establish methodologies for system testing, conduct penetration testing and source code review, and enable recovery measures and user access controls;
- Board and senior management of regulated entities are to: (a) ensure appropriate accountability structure and organisational risk culture is in place, and (b) be trained in technology risk and cybersecurity;
- Notify the MAS of breaches of security and confidentiality of financial institutions' customer information (MAS Notices and Guidelines on Technology Risk Management and the MAS Guidelines on Outsourcing); and
- Implement cybersecurity measures to protect IT systems, and prevent and mitigate against

malware infection or attacks (MAS Notices on Cyber Hygiene).

### 6. Sanctions & non-compliance

#### Administrative sanctions:

Cybersecurity Act 2018:

- Fines not exceeding SGD 10,000 for each contravention of Part 5 of the Cybersecurity Act 2018 by a licensee, which contravention is not an offence or non-compliance with any license conditions, but not exceeding SGD 50,000 in aggregate.
- Fines not exceeding SGD 100,000 for non-participation in a cybersecurity exercise as directed in writing by the Commissioner of Cybersecurity.

#### Criminal sanctions:

Cybersecurity Act 2018:

- Varies depending on the specific offence, although in general a criminal fine not exceeding SGD 100,000 or imprisonment for a term not exceeding two to ten years or both.

CMA**:**

- A criminal fine not exceeding SGD 50,000 or imprisonment for a term not exceeding ten years or both; and
- In respect of protected computers, a criminal fine not exceeding SGD 100,000 or imprisonment for a term not exceeding 20 years or both.

#### Others:

CMA:

- Compensation for damage caused to computer, programme or data.

MAS Rules:

- Varies depending on the type of regulatory instrument that set out the specific rules (e.g. directives, guidelines, notices or circulars). For example, the contravention of guidelines is not a criminal offence and does not attract civil penalties but may have an impact on the regulator's overall risk assessment of that entity and renewal of licences issued by the regulator. Circulars, on the other hand, are documents sent for the relevant entities' information and have no legal effect. Notices primarily impose legally binding requirements on a specified class of financial institutions or persons.

### 7. Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?

Yes, the Singapore Computer Emergency Response Team (SingCERT) responds to cybersecurity incidents for its Singapore constituents. It was set up to facilitate the detection, resolution and prevention of cybersecurity related incidents on the Internet.

### 8. National cybersecurity incident management structure

According to Singapore’s Cybersecurity Strategy, the National Cyber Security Centre (part of the CSA) will coordinate with sector regulators to provide a national level response and facilitate quick alerts to cross-sector threats.

### 9. Other cybersecurity initiatives

Singapore's Cybersecurity Strategy sets out Singapore's vision, goals and priorities for cybersecurity. It engenders coordinated action and facilitates international partnerships for a resilient and trusted cyber environment.

New Advisories and Guidelines, published in 2024 and 2025, include the following:

- Guidelines and Companion Guide on Securing AI Systems (published in October 2024)
- Advisory on Software Bill of Materials and Real-time Vulnerability Monitoring for Open-Source Software and Third-Party Dependencies (published in February 2025)

**10. Useful links**

Cybersecurity Act 2018

Computer Misuse Act 1993

Summary of the proposed amendments to the Cybersecurity Act 2018

Public consultation on the proposed amendments to the Cybersecurity Act 2018

Press release on the proposed amendments to the Computer Misuse Act 1993

Singapore Cybersecurity Strategy 2021

MAS Rules

## Key Contacts


Sheena Jacob
Singapore
Partner


## Authors


Sheena Jacob
Singapore
Partner

Andre Choo
Singapore
Associate
Holborn Law LLC

Adel Hamzah
Associate
left_cms