
CHAMBERS GLOBAL PRACTICE GUIDES

Data Protection & Privacy 2026

Definitive global law guides offering
comparative analysis from top-ranked lawyers

**Singapore: Law & Practice
and Trends & Developments**

Chong Kin Lim, David N. Alfred and Anastasia Chen
Drew & Napier LLC



SINGAPORE



Law and Practice

Contributed by:

Chong Kin Lim, David N. Alfred and Anastasia Chen
Drew & Napier LLC

Contents

1. Legal and Regulatory Framework p.4

- 1.1 Overview of Data and Privacy-Related Laws p.4
- 1.2 Rights and Obligations p.5
- 1.3 Special Categories of Personal Data p.7
- 1.4 Processing of Personal Data for Research and Development Purposes p.8
- 1.5 Processing of Personal Data in the Context of Artificial Intelligence p.9
- 1.6 Data Breach Requirement p.10
- 1.7 Regulators p.11
- 1.8 Enforcement Proceedings and Fines p.11
- 1.9 Enforcement Trends p.13

2. Privacy Litigation p.13

- 2.1 Privacy Litigation Overview p.13
- 2.2 Recent Case Law p.14
- 2.3 Collective Redress Mechanisms p.14

3. Requirements for the Protection and Processing of Non-Personal Data p.14

- 3.1 Objectives and Scope of Data Regulation p.14
- 3.2 Interaction of Data Regulation and Data Protection p.15
- 3.3 Rights and Obligations Under Applicable Data Regulation p.15
- 3.4 Regulators and Enforcement p.15

4. Sectoral Topics p.15

- 4.1 Use of Cookies p.15
- 4.2 Personalised Advertising and Other Online Marketing Practices p.16
- 4.3 Employment Privacy Law p.16
- 4.4 Data Protection in M&A p.16

5. International Considerations p.17

- 5.1 Restrictions on International Data Transfers p.17
- 5.2 Government Notifications and Approvals p.18
- 5.3 Data Localisation Requirements p.18
- 5.4 Blocking Statutes p.18
- 5.5 Recent Developments p.18

Drew & Napier LLC established a dedicated Data Protection, Privacy and Cybersecurity Practice to leverage its unrivalled experience in data privacy and data and cyber governance and offer clients best-in-class solutions to address their legal and compliance needs in Singapore and across the region. The firm represents many regional companies, multinationals, industry associations, government bodies and regulators, and regularly assists them on a wide range of matters in Singapore and ASEAN member countries.

At the forefront of data protection law in Singapore since 2013, the Data Protection, Privacy & Cybersecurity Practice Group has worked on significant data protection enforcement cases and appeals, including those involving cybersecurity elements. Building on its experience in this field, the Drew Data Protection & Cybersecurity Academy was established in 2020 to offer clients services relating to data protection and cybersecurity compliance, including training, consulting and external data protection officer services.

Authors



Chong Kin Lim heads Drew & Napier's highly regarded TMT practice group. His clients include telecoms and media regulators, global carriers, technology market leaders, global broadcasters and content providers.

Chong Kin has worked on every significant development in the Singapore TMT market, and continues to play a key role in the development of sectoral competition regulation in Singapore. He was the lead external counsel in the liberalisation of the telecommunications, media and postal sectors, and has assisted regulators in conceptualising and drafting "first-of-its-kind" sectoral competition legislation and frameworks.



David N. Alfred is a director of Drew & Napier LLC and co-head of the firm's Data Protection, Privacy & Cybersecurity Practice Group. He is concurrently co-head and programme director of the Drew Data Protection &

Cybersecurity Academy. David is a data protection, cybersecurity and technology lawyer with over 25 years' experience advising on a broad range of matters relating to digital technology, telecommunications and the internet. He has substantial experience advising on data protection and cybersecurity compliance, regulatory enforcement, data breaches and international aspects of data protection. Prior to joining the firm, David was the first Chief Counsel of Singapore's data protection authority, the Personal Data Protection Commission.



Anastasia Chen is a director of Drew & Napier LLC and deputy head of the firm's Data Protection, Privacy & Cybersecurity Practice Group. Prior to joining the firm, Anastasia was Deputy Chief Counsel to Singapore's

Personal Data Protection Commission (PDPC) and Info-communications Media Development Authority (IMDA) for over nine years, during which she served as lead counsel for PDPC's matters, IMDA's procurement and intellectual property portfolios, as well as IMDA's Data Administration Group. She has received accolades from legal publications, with clients commending her deep industry and regulatory expertise, as well as legal acumen, especially when dealing with novel problems.

Drew & Napier LLC

10 Collyer Quay
10th Floor
Ocean Financial Centre
Singapore 049315

Tel: +65 6531 4110
Fax: +65 6535 4864
Email: mail@drewnapier.com
Web: www.drewnapier.com



1. Legal and Regulatory Framework

1.1 Overview of Data and Privacy-Related Laws

Singapore's data protection framework is laid out in the Personal Data Protection Act 2012 (PDPA), which is the main statute governing the collection, use, disclosure and care of personal data in the private sector. Oversight, administration and enforcement of the PDPA are vested in the Personal Data Protection Commission (PDPC).

The core data protection obligations are set out in Parts 3 to 6A of the PDPA. These provisions regulate, among other matters, the collection, use, disclosure, access, correction, accuracy security, retention, overseas transfer of personal data and notification of data breaches (collectively, the "Data Protection Provisions"). In addition, Parts 9 and 9A of the PDPA establish Singapore's national Do Not Call (DNC) Registry, and set out the duties imposed on organisations in relation to the transmission of specified marketing communications to Singapore telephone numbers.

The PDPA was updated through the Personal Data Protection (Amendment) Act 2020. The majority of the significant amendments, including mandatory data breach notifications and new consent-related provisions, took effect on 1 February 2021.

The PDPA has both territorial and extraterritorial effect, applying to all organisations that are not a public agency, whether or not formed or recognised under

the laws of Singapore, or resident or having an office or a place of business in Singapore.

The PDPA is supplemented by subsidiary regulations, including the following:

- Personal Data Protection Regulations 2021 (the "PDP Regulations"), which address matters such as data transfers out of Singapore and procedures relating to access and correction requests;
- Personal Data Protection (Enforcement) Regulations 2021 (the "Enforcement Regulations"), which govern enforcement processes and powers;
- Personal Data Protection (Notification of Data Breaches) Regulations 2021, which prescribe thresholds and timelines for mandatory breach notification;
- Personal Data Protection (Composition of Offences) Regulations 2021;
- Personal Data Protection (Appeal) Regulations 2021; and
- Personal Data Protection (Do Not Call Registry) Regulations 2013.

These regulations are legally binding and are issued pursuant to the PDPA.

The PDPA operates alongside sectoral laws and regulations that set out further data protection and cybersecurity obligations for the compliance of regulated entities. Some examples include:

- Healthcare Services Act 2020 (No 3 of 2020) (HCSA), addressing the confidentiality and retention of medical records;
- Code of Practice for Competition in the Provision of Telecommunication Services 2012 issued under the Telecommunications Act 1999 (2020 Revised Edition), regulating how telecommunications licensees may handle end-user service information; and
- Banking Act 1970 (2020 Revised Edition), containing statutory banking secrecy obligations governing the disclosure and handling of customer information by banks.

Additionally, the PDPC has issued a substantial body of advisory guidelines. While these guidelines are not legally binding, they play an important interpretive role by explaining how the PDPC understands and applies the PDPA in practice, and they are frequently relied upon by organisations seeking compliance certainty.

See **3.1 Objectives and Scope of Data Regulation** and **1.5 Processing of Personal Data in the Context of Artificial Intelligence** on how the PDPA interacts with laws governing non-personal data and AI respectively.

1.2 Rights and Obligations

Primary Obligations

The PDPA generally imposes 11 primary obligations on organisations.

Consent obligation

Generally, an organisation may not collect, use or disclose personal data unless the individual has given consent or is deemed to have consented under the PDPA. However, consent is not required where the collection, use or disclosure is authorised or mandated by written law.

The PDPA recognises a number of exceptions where personal data may be processed without consent. These include situations involving:

- the protection of vital interests;
- matters of public interest;
- an organisation's legitimate interests;
- business asset transactions;
- business improvement purposes; and

- research.

Purpose limitation obligation

Personal data may only be collected, used or disclosed for purposes that a reasonable person would consider appropriate in the circumstances. Where required under the PDPA, those purposes must also be made known to the individual.

Notification obligation

Organisations are generally required to inform individuals of the purposes for which their personal data is being collected, used or disclosed. Notification is not necessary where consent is deemed by conduct or contractual necessity in accordance with the PDPA or where processing without consent is permitted pursuant to an exception to consent under the PDPA (save that there are disclosure/notification requirements when relying on the exceptions relating to general legitimate interests and managing employees).

Access obligation

Upon request, an organisation must provide an individual with access to their personal data in the organisation's possession or control, as well as information about how that data has been used or disclosed. The obligation is subject to exceptions set out in the Fifth Schedule to the PDPA, including circumstances where disclosure would compromise an ongoing investigation. There are also specific circumstances where access is prohibited. Further details are set out under "Data Subject Rights" below.

Correction obligation

Organisations must, on request, correct inaccuracies or omissions in an individual's personal data, unless there are reasonable grounds for refusing the correction or the request falls within one of the prescribed exceptions in the Sixth Schedule to the PDPA. Further details are set out under "Data Subject Rights" below.

Accuracy obligation

Where personal data is likely to be used to make a decision affecting an individual, or disclosed to another organisation, reasonable steps must be taken to ensure that the data is accurate and complete. This obligation is context-specific and turns on what is reasonable in the circumstances.

Protection obligation

Organisations are required to implement reasonable security arrangements to safeguard personal data in their possession or under their control. These measures must protect against unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

Retention limitation obligation

Personal data must not be retained for longer than is necessary to fulfil the purposes for which it was collected. Once those purposes are no longer served, and retention is no longer required for legal or business reasons, the data must be deleted or anonymised.

Transfer limitation obligation

An organisation may only transfer personal data outside Singapore if it ensures that the recipient jurisdiction provides a level of protection comparable to that under the PDPA.

Data breach notification obligation

In the event of a data breach, an organisation must conduct an assessment to determine whether the breach is notifiable under the PDPA. Where notification is required, the organisation must notify the Personal Data Protection Commission (PDPC) as soon as practicable and, in any event, no later than three calendar days after making the assessment. In specified cases, affected individuals must also be informed.

Accountability obligation

Finally, organisations must be able to demonstrate compliance with the PDPA. This includes appointing a data protection officer, developing and implementing internal data protection policies and practices, and embedding data protection considerations into organisational governance and operations.

Data Subject Rights

The PDPA confers a limited set of rights on individuals in relation to their personal data. These rights include the ability to withdraw consent to data processing, to request access to personal data held by organisations, and to seek the correction of inaccuracies or omissions in such data.

Right of access to personal data

Under Section 21 of the PDPA, individuals have the right to request access to personal data about them that is in the possession or under the control of an organisation, as well as information about how that data has been used or disclosed within the preceding year. However, access is prohibited under the following circumstances pursuant to Section 21 (3) of the PDPA:

- threaten the safety or health of another individual;
- cause immediate or grave harm to the safety or health of another individual;
- reveal another individual's personal data;
- disclose the identity of an individual who provided personal data, without that individual's consent; or
- be contrary to national interest.

Furthermore, an organisation is not obliged to provide access to an individual's personal data or related information where the request falls within the situations set out in the Fifth Schedule to the PDPA.

Right to correction

Under Section 22 of the PDPA, individuals may request the correction of errors or omissions in their personal data. Where a correction is made, the organisation is generally required to send the corrected data to other organisations to which it was disclosed within the preceding year, unless this is unnecessary for legal or business purposes. The correction right does not extend to opinion data or derived personal data, and is subject to exceptions set out in the Sixth Schedule to the PDPA.

Right to withdraw consent

Under Section 16 of the PDPA, individuals may, upon giving reasonable notice, withdraw any consent (including deemed consent) previously given for the collection, use or disclosure of their personal data. Following withdrawal, the organisation must cease the relevant processing activity unless continued processing without consent is authorised or required under the PDPA or other written law.

Right to object to marketing

See detail set out under "Right to withdraw consent".

Individuals may also object to the receipt of specified marketing messages by registering their Singapore telephone numbers with one or more of the national DNC Registers. Registration restricts the sending of telemarketing messages to those numbers, unless clear and unambiguous consent to the sending of the telemarketing message is obtained in evidential form.

Right to lodge complaints

Individuals may lodge complaints with the PDPC in respect of alleged breaches of the PDPA. The PDPC may facilitate resolution, refer the matter for mediation, or conduct a formal investigation and take enforcement action where appropriate.

Main Compliance Requirements for Organisations

The following are the main compliance requirements.

Establish data protection governance

- Appoint a Data Protection Officer (DPO) and make the DPO's business contact details publicly available.
- Adopt and maintain written data protection policies and documented practices/processes to ensure the organisation complies with the PDPA.

Understand and manage personal data holdings

- Identify and document personal data assets and data flows across the organisation.
- Assess key data protection risks and compliance gaps (including in existing systems and processes).

Implement basic operational controls

- Put in place procedures for handling access, correction and consent withdrawal requests.
- Implement reasonable technical and organisational security measures to protect personal data.
- Establish retention and disposal practices to prevent unnecessary retention of personal data.

Prepare for data breaches and complaints

- Establish a data breach response plan and designate a response team.
- Implement internal escalation and assessment procedures for suspected data breaches.
- Put in place a basic complaint-handling process for data protection matters.

Train staff and raise awareness

- Provide periodic training to employees who handle personal data.
- Communicate internal policies and expectations relating to personal data protection.

Review and maintain compliance

- Conduct periodic reviews of data protection policies and practices.
- Test breach response readiness (eg, through table-top exercises).
- Consider data protection impact assessments for new or significantly changed systems or uses of data.

1.3 Special Categories of Personal Data Processing of Health Data

The PDPA does not designate health data as a separate statutory category of "special" personal data. However, health and medical information is generally regarded as particularly sensitive, and its processing is subject to heightened expectations under the PDPA, as supplemented by sector-specific guidance and legislation.

The collection, use and disclosure of health data are governed primarily by the general PDPA obligations. PDPC has issued the Advisory Guidelines for the Healthcare Sector (Revised 20 September 2023), which provide practical guidance on how these obligations apply in common healthcare scenarios. The guidelines address, among other matters:

- the role of consent in clinical care;
- circumstances where processing without consent may be permitted; and
- the handling of access and correction requests relating to medical records.

Organisations handling health data are expected to implement stronger security and access controls, reflecting the sensitivity of such data, and to ensure that collection and use are limited to what is reasonably necessary for healthcare or related purposes. Retention of medical records must also be justified by ongoing care needs, legal requirements or professional standards.

In addition to the PDPA, healthcare providers are subject to sector-specific statutory requirements. The HCSA, the Healthcare Services (General) Regulations 2021, and applicable licensing conditions impose obligations relating to patient confidentiality and record-keeping, which operate alongside the PDPA framework.

Processing of Data Relating to Minors

The processing of minors' personal data is governed by the Data Protection Provisions, as supplemented by guidance issued by the PDPC.

The principal requirement concerns consent. Whether a minor may validly consent depends on whether the minor has sufficient understanding of the nature and consequences of the collection, use or disclosure of personal data. The PDPC has indicated that, as a general benchmark, minors aged 13 years and above are typically capable of providing valid consent on their own behalf. Where an organisation has reason to believe that a minor lacks such understanding, consent must be obtained from a parent or legal guardian.

For online products or services likely to be accessed by children (individuals below 18 years of age), the PDPC's Advisory Guidelines on the PDPA for Children's Personal Data in the Digital Environment impose additional expectations. In particular, organisations must ensure that privacy notices and consent mechanisms are age-appropriate and readily understandable, and that children aged between 13 and 17 years understand the consequences of giving and withdrawing consent.

Children's personal data is generally regarded by the PDPC as sensitive, necessitating stronger protection. The use of such data or profiles to target harmful or inappropriate content (as defined in the Code of Practice for Online Safety, issued under the Broadcasting Act 1994) is considered unreasonable. Organisations are also expected to implement enhanced safeguards and to assess data protection risks, such as through data protection impact assessments, where products or services are likely to involve children's data.

Processing of Data Relating to Criminal Convictions and Investigations

The processing of personal data relating to criminal convictions and investigations is subject to the Data Protection Provisions. Under the PDPA, processing data without consent is permitted where it is necessary for purposes such as:

- investigations or proceedings;
- compliance with written law; or
- where required by public authorities exercising lawful functions.

Further, where an organisation has provided personal data to a prescribed law enforcement authority without the individual's consent, the PDPA requires the organisation to refrain from notifying the individual of that disclosure. Personal data gathered in connection with investigations, prosecutions or related proceedings may fall outside the access regime under the PDPA, particularly while proceedings remain pending. In such circumstances, access to the data should generally be pursued through the relevant criminal or civil discovery processes, which operate independently of the PDPA framework.

1.4 Processing of Personal Data for Research and Development Purposes

Generally, the PDPC promotes the use of anonymisation as a means of tapping on data for insights where individuals need not be identified.

In Singapore, the PDPC defines anonymisation as the process of "converting personal data into data that cannot identify any particular individual". A dataset would be considered anonymised, where there is no serious possibility that an individual can be identified from the dataset when it is combined with other information that the data recipient has or is likely to have access to, by carrying out an assessment of the risk of re-identification. The following factors go towards lowering re-identification risks:

- the intended use of the anonymised data and the extent of its disclosure are controlled, for example where the data is used internally or disclosed only to a restricted group of recipients rather than made publicly available;

- access to the anonymised data is limited to recipients who do not possess special knowledge of the individuals concerned, or who do not have access to complementary information that could reasonably be used to re-identify individuals;
- the recipient does not have both the ability and motivation to re-identify individuals from the dataset, or where such risks are mitigated through appropriate legal or regulatory safeguards; or
- the anonymised dataset can reasonably be expected to remain anonymised over time, having regard to foreseeable technological developments, data availability and data-linking techniques.

However, where the nature of data is highly sensitive to individuals (eg, records of individuals with HIV), even if the organisation assesses that there is a less than serious possibility of an individual being re-identified from the data, PDPC has cautioned organisations to carefully consider whether using or disclosing such data would be appropriate.

Once data is anonymised, such that individuals can no longer be identified, it no longer falls under the PDPA. Therefore, this could allow medical device or software providers to use such anonymised data for research and development without patient consent. Organisations should note that, if the risk of re-identification is more than a serious possibility, the data is brought back under the Data Protection Provisions, such as obtaining consent subject to approved exceptions.

Impact of the European Health Data Space Regulation (EHDS)

The EHDS regime is designed to govern entities operating within the EU health data ecosystem, and its core obligations apply mainly to health data holders established in the EU. Singapore-based companies may be directly subject to the EHDS if they have an established presence within the EU, and where they fall within the definition of a health data holder as entities developing health-related products or services, and wellness applications, or conducting healthcare-related research – and, in that capacity, either process personal electronic health data as a controller or have the ability to make non-personal electronic health data available through control of the relevant technical systems.

Singapore life sciences companies may also be indirectly affected where they operate EU subsidiaries, collaborate with EU healthcare providers or research institutions, or supply digital health products, medical devices or Electronic Health Record (EHR)-linked services into the EU market. In such cases, EU-based affiliates or partners may be required to comply with EHDS obligations on data access, secondary use and secure processing, which can flow down contractually to Singapore parent entities or vendors. In contrast, Singapore companies seeking to access EU health datasets for research or product development will generally not qualify as health data users under the EHDS unless Singapore is recognised by the EU as offering reciprocal access. However, this has not occurred to date.

Domestically, Singapore parliament has passed the Health Information Bill, which aims to structure national data sharing through the National Electronic Health Record System, mirroring the EHDS.

1.5 Processing of Personal Data in the Context of Artificial Intelligence

There is currently no AI-specific legislation in Singapore. The PDPA applies to the processing of personal data throughout the development, training, testing, deployment and operation of AI systems. While the PDPA does not contain provisions specifically tailored to AI, organisations deploying AI systems that collect, use or disclose personal data must comply with all obligations in the PDPA, such as the consent (Sections 13 to 20 of the PDPA), notification (Section 20 of the PDPA) and accountability (Sections 11 and 12 of the PDPA) obligations.

On 1 March 2024, the PDPC issued the Advisory Guidelines on the Use of Personal Data in AI Recommendation and Decision Systems, which articulate a risk-based approach to AI governance and provide targeted guidance on how the PDPA applies in AI contexts. These guidelines emphasise that consent and notification obligations must operate together to ensure that individuals are meaningfully informed when their personal data is used in AI-driven features or automated decision-making.

Organisations are expected, where practicable, to provide a clear explanation of:

- the function of the AI system of the product that utilises personal data;
- a general description of categories of personal data to be collected and processed;
- an explanation on how such data supports or influences the product feature; and
- the specific data features likely to affect the product feature.

Where detailed explanations cannot be provided due to legitimate commercial sensitivity or security concerns, organisations are expected to document and justify such limitations internally.

Under the PDPA's accountability obligation, organisations must implement internal governance measures to ensure that AI-assisted decisions are fair and reasonable. This includes maintaining policies, risk controls and review mechanisms appropriate to the context in which the AI system is used. The degree of transparency and oversight expected is risk-proportionate, taking into account factors such as:

- the potential impact on individuals;
- the sensitivity of the data involved; and
- the extent to which decisions are automated without human involvement.

There are currently no legally prohibited AI use cases or formally designated "high-risk" AI categories under data protection law.

The Info-communications Media Development Authority (IMDA) and the PDPC have jointly issued the Model Artificial Intelligence Governance Framework. It is a voluntary but influential instrument that encourages organisations to align their internal governance, policies and practices with recognised data protection standards, including the PDPA and international principles such as the OECD Privacy Principles.

1.6 Data Breach Requirement

Under the PDPA, a data breach occurs when personal data is accessed, collected, used, disclosed, copied, modified or lost without authorisation, or when there is

a loss of a storage medium containing personal data in circumstances that make such outcomes likely. Organisations must expeditiously determine whether a data breach meets the threshold for notification, generally performing this assessment as soon as possible and typically within 30 days of becoming aware of the incident.

Where a breach is deemed notifiable, the organisation must report it to the PDPC within three days of making that determination. A breach is notifiable if it either (i) causes, or is likely to cause, significant harm to affected individuals, or (ii) affects 500 or more individuals. Once notification to the PDPC has been made, if the breach involves actual or potential significant harm to individuals, organisations are generally required to inform the affected individuals promptly.

The following are practical steps to be taken by organisations when a data breach occurs.

- *Immediate containment* – For example, secure affected systems and data to prevent further unauthorised access.
- *Assessment of risk* – Determine the scope of the breach, the type of personal data involved and the potential harm to individuals.
- *PDPC notification* – If the breach is notifiable, submit a report to the PDPC within three days of determination.
- *Notification of individuals* – Where significant harm is likely or has occurred, communicate with affected individuals in a clear and timely manner.
- *Remediation and prevention* – Address system vulnerabilities, review policies and procedures, and implement measures to reduce the likelihood of recurrence.

If a data processor suspects that a breach has occurred in relation to personal data it handles on behalf of a data controller, it must alert the controller swiftly. The controller is then responsible for evaluating whether the incident meets the notifiable threshold and for co-ordinating any required reporting to the PDPC and affected individuals.

Notifiable breaches may trigger investigations by the PDPC, which has the authority to examine the

organisation's breach response and data protection practices, potentially resulting in enforcement action. In addition, data breaches expose organisations to potential privacy litigation, outlined in **2. Privacy Litigation**.

1.7 Regulators

The PDPC is the primary regulator of the PDPA. Its jurisdiction covers private sector organisations. Its core functions include:

- promoting awareness of data protection in Singapore;
- providing advisory, consultancy and technical services relating to data protection;
- advising the Singapore government on policy and representing Singapore internationally;
- conducting research and educational programmes;
- facilitating technical co-operation and exchange in the area of data protection with other organisations, including foreign data protection authorities and international or intergovernmental organisations, on its own behalf or on behalf of the government; and
- administering and enforcing the PDPA and functions assigned by law or the Minister.

Investigations may arise from complaints or on the PDPC's own initiative. According to the Advisory Guidelines on Enforcement of the Data Protection Provisions, the PDPC would consider factors such as:

- whether the organisation may have breached all or a substantial portion of its obligations under the PDPA;
- whether the organisation's actions reflect a systemic lapse in compliance, including a failure to put in place or maintain adequate internal policies and procedures to ensure adherence to the PDPA;
- the number of individuals who have been, or could potentially be, affected by the organisation's actions;
- the extent of harm or adverse impact suffered by the complainant or any affected individuals;
- whether the organisation has a history of PDPA contraventions or has failed to take adequate remedial steps to prevent a recurrence of earlier breaches;

- whether the complainant had previously sought to resolve the matter directly with the organisation without success;
- where the PDPC has attempted to facilitate dispute resolution, whether the parties agreed to participate, their conduct throughout the process, and the eventual outcome of such resolution efforts;
- where the PDPC has initiated a review, whether the organisation complied with its obligations under the Enforcement Regulations, its conduct during the review, and the result of that review; and
- broader considerations of public interest.

In the course of investigations, the PDPC may:

- compel the production of documents and information;
- compel witnesses, and conduct oral examinations or record statements; and
- enter premises to take necessary equipment or copies of documents (amongst other things).

1.8 Enforcement Proceedings and Fines

The PDPC is responsible for enforcing the PDPA. It is guided by four key objectives as set out in the PDPC's Guide to Active Enforcement (revised on 1 October 2022), namely:

- to respond to PDPA breaches effectively, with attention to incidents affecting large numbers of individuals or involving personal data that may result in significant harm;
- to apply enforcement measures in a manner that is proportionate and consistent across organisations found to be in breach of the PDPA;
- where penalties imposed function as a meaningful deterrent against future non-compliance; and
- to ensure that organisations in breach take adequate remedial action to rectify weaknesses in the protection and handling of personal data within their possession or control.

When a possible personal data incident comes to the PDPC's attention (whether through a complaint, self-report or other means), the PDPC will first assess whether the matter warrants a formal investigation. The Commissioner may decide not to investigate where:

- the issue is more appropriately resolved through facilitation or mediation;
- the facts do not suggest a breach of the data protection obligations; or
- the organisation concerned falls primarily within the remit of another sectoral regulator better placed to address the matter.

If investigation is warranted, the PDPC formally opens a case. During an investigation, the PDPC may:

- issue notices for the production of documents and information from the relevant organisations;
- carry out interviews and record statements from the organisations and individuals concerned; and
- where appropriate, undertake site visits to obtain a comprehensive understanding of the facts.

The organisation under investigation is given the opportunity to respond and make representations before any decision is reached.

After evaluating the facts of the case and representations, the PDPC determines whether a breach has occurred and may issue directions to the organisation. These may include financial penalties, which currently can reach SGD1 million or 10% of the organisation's annual turnover in Singapore, whichever is higher.

When setting financial penalties, the PDPC considers factors such as:

- the nature, gravity and length of the organisation's or individual's non-compliance;
- the type and sensitivity of the personal data affected by the non-compliance;
- whether the organisation or individual derived any financial gain, or avoided a financial loss, as a result of the non-compliance;
- the steps taken by the organisation or individual to reduce or address the impact of the non-compliance, including how promptly and effectively those steps were implemented;
- whether, notwithstanding the non-compliance, the organisation or individual had put in place appropriate and sufficient measures to comply with the PDPA;

- any history of previous non-compliance with the PDPA by the organisation or individual;
- the extent to which the organisation or individual complied with any directions issued under Section 48I or 48L(4) to remedy or mitigate the effects of the non-compliance;
- whether the proposed financial penalty is appropriate and effective in promoting compliance and deterring future breaches of the PDPA;
- the anticipated impact of the financial penalty on the organisation or individual, including their ability to continue normal operations; and
- any other factors considered relevant.

Beyond financial penalties, the PDPC may issue administrative directions to compel compliance, including requiring organisations to cease unlawful data practices, correct or delete personal data, or provide access to affected individuals, with such directions enforceable through the courts. Separately, the PDPA also recognises a private right of action for individuals who suffer loss or damage.

An organisation or individual dissatisfied with a direction or decision of the PDPC may first apply to the PDPC for reconsideration, under Section 48N of the PDPA. Following a reconsideration decision, the aggrieved party may appeal to the Data Protection Appeal Panel pursuant to Section 48Q of the PDPA. Alternatively, an appeal may be brought directly to the Appeal Panel without first seeking reconsideration.

A further appeal from a decision of the Appeal Panel lies to the High Court only on limited grounds, namely a question of law or, in the case of a financial penalty, the amount imposed. Applications for reconsideration and appeals must be made within the prescribed period of 28 days.

Illustrative Example

In *Re Marina Bay Sands Pte Ltd* [2025] SGPDP 6, the PDPC imposed a financial penalty of SGD315,000 on Marina Bay Sands Pte Ltd. This decision illustrates the PDPC's calibrated approach to financial penalties following the 2020 amendments to the PDPA, clarifying that penalties are assessed with reference to factors such as the organisation's annual turnover, the seriousness and duration of the breach, and the extent

of harm or risk posed to individuals, rather than being applied mechanically at the statutory maximum.

Criminal Offences

Section 51 (1) of the PDPA provides for specific criminal offences for persons, including requesting access to, or correction of, another individual's personal data without authority. Under Section 51 (3) of the PDPA, criminal offences for both persons and organisations include:

- evading access/correction requests;
- obstructing enforcement; or
- providing false information to the Commission, an inspector or an authorised officer.

Offenders are liable to fines and/or imprisonment.

Further, Part 9B of the PDPA introduces specific offences targeting egregious mishandling of personal data at the individual level. These provisions make it a criminal offence for an individual to knowingly or recklessly:

- disclose personal data without authorisation;
- use personal data to obtain a wrongful gain or cause harm or loss to another person; or
- re-identify anonymised information without authority.

Individuals convicted of such offences may be subject to fines of up to SGD5,000, imprisonment for up to two years, or both.

1.9 Enforcement Trends

Most enforcement actions taken by the PDPC continue to arise from inadequate data security practices, with breaches of the Protection Obligation forming the largest share of decisions issued in the past 24 months.

On 28 October 2025, the PDPC levied a financial penalty of SGD315,000 against Marina Bay Sands Pte Ltd (MBS) in *Re Marina Bay Sands Pte Ltd [2025]* SGP-DPC 6. This represents the second-largest single fine imposed since the PDPA took effect, and the highest penalty issued following the 2021 PDPA amendments, which raised the maximum financial penalty

from SGD1 million to up to 10% of an organisation's annual turnover in Singapore (subject to a minimum of SGD1 million).

In October 2023, the personal data of approximately 665,000 MBS patrons was unlawfully accessed and exfiltrated, with the compromised information later offered for sale on the dark web. The breach arose from deficiencies during a major software migration in March 2023, where critical security configurations were compiled by a single employee without adequate oversight or verification. The PDPC found that MBS failed to implement reasonable security measures and appropriate post-migration controls, constituting a negligent breach of the protection obligation, particularly given MBS's scale and available resources.

This decision is significant for articulating a structured penalty framework, confirming that, while the enhanced maximum fines introduced in 2021 provide the PDPC with greater headroom, penalties remain proportionate and fact-specific. The PDPC has also emphasised accountability, looking closely at whether organisations had reasonable governance measures, risk assessments and security practices in place prior to an incident.

The decision highlights that organisations must implement robust, layered governance and verification controls, particularly for high-risk activities such as large-scale system migrations, rather than relying solely on individual employees. It also signals the PDPC's increasing focus on deterrence under the enhanced penalty framework, with significant fines possible even where the data involved is not highly sensitive, underscoring the need to prioritise security by design and proactive compliance.

2. Privacy Litigation

2.1 Privacy Litigation Overview

In Singapore, the bulk of data protection enforcement occurs through regulatory measures by the PDPC rather than civil proceedings in the courts.

Under Section 48O(1) of the PDPA, a person who suffers loss or damage directly arising from a contraven-

tion of specified PDPA provisions may bring a private civil action against the organisation in court, without first obtaining a finding from the PDPC. Recent decisions, including the High Court's ruling in *Piper, Martin v Singapore Kindness Movement* [2025] SGHC 173 (*Piper, Martin*) and *Reed, Michael v Bellingham, Alex (Attorney-General, intervener)* [2022] SGCA 60 (*Reed*), illustrate the approach taken by the courts. Claimants must establish a statutory breach, causation, and actionable loss and damage. Crucially, the Court in *Piper, Martin* emphasised that a "strict causal link" must be established in order for a claim for loss or damage to succeed. Under Section 48O(3), the court may grant injunctive or declaratory relief, award damages, or order any other appropriate remedy.

While the PDPC itself cannot award compensation, non-material harm is compensable in civil proceedings. However, the Singapore courts take a cautious approach towards awarding non-material damages. The Court of Appeal in *Reed* emphasised that courts assess such harm on a fact-specific basis, considering (among other things):

- the sensitivity of the personal data involved;
- the nature and duration of the breach;
- the defendant's conduct (eg, negligent versus malicious);
- the risk of future misuse; and
- the actual impact on the claimant.

2.2 Recent Case Law

Recent case law has clarified key contours of data protection litigation in Singapore, where court actions remain relatively limited. In *Piper, Martin v Singapore Kindness Movement* [2025] SGHC 173, the High Court clarified the parameters of "deemed consent" and the investigation exception under the PDPA, holding that disclosures of personal data must be objectively necessary and reasonable for the stated purpose, even in the context of internal investigations. See **2.1 Privacy Litigation Overview** for the Court's holding on requirements for loss or damages claims to succeed.

Read together with *Reed*, these decisions establish that while non-material harm such as emotional distress can be compensable, mere loss of control over

personal data is insufficient, and liability will turn on necessity, proportionality and proof of actual impact.

2.3 Collective Redress Mechanisms

Singapore does not provide collective redress mechanisms to safeguard the shared interests of multiple individuals.

3. Requirements for the Protection and Processing of Non-Personal Data

3.1 Objectives and Scope of Data Regulation

Singapore currently has no dedicated legislation specifically regulating non-personal data or cross-sector data access comparable to the EU Data Act. The governance of technologies such as IoT, cloud computing and other data processing services falls primarily under the broader PDPA and the Cybersecurity Act 2018, alongside sector-specific guidance from agencies such as the IMDA.

The Data Protection Provisions continue to apply to IoT devices and other connected services that collect personal data, ensuring that organisations deploying such technologies maintain responsible data management practices.

Further, the Amendment Act will introduce a new data portability obligation, which requires an organisation, upon an individual's request, to transfer the individual's personal data in its possession or control (including data generated through IoT and connected devices) to another organisation in a commonly used, machine-readable format. However, it is not yet in force.

Data intermediaries processing data on behalf of others are also subject to specific obligations under the PDPA, namely the protection obligation, the retention limitation obligation, and the data breach notification obligation (where a data intermediary becomes aware, or has reasonable grounds to suspect, that a data breach has occurred involving personal data it processes for another organisation, it is required to inform that organisation promptly).

3.2 Interaction of Data Regulation and Data Protection

See **1.1 Overview of Data and Privacy-Related Laws**.

3.3 Rights and Obligations Under Applicable Data Regulation

In Singapore, there is no legislation specifically regulating the use of IoT or other non-personal data services beyond existing frameworks for personal data. Key obligations under the PDPA, set out in **3.1 Objectives and Scope of Data Regulation**, continue to apply where personal data is involved, and organisations must implement measures to ensure compliance.

The PDPC issued a Guide to Data Sharing (revised 1 February 2018), which provides guidance on the sharing of personal data:

- within the organisation or group of organisations;
- with a data intermediary; and
- with one or many organisations.

Specifically, compliance with the following are key issues that would arise in the context of data sharing:

- consent obligation;
- purpose limitation obligation;
- notification obligation; and
- transfer limitation obligation.

The IMDA's Internet of Things Cyber Security Guide (published March 2020) for IoT services provides practical obligations for developers, providers and enterprise users, focusing on security principles, risk management and operational best practices, though it explicitly excludes privacy matters. Organisations deploying IoT or cloud-based systems should integrate these baseline security measures with PDPA obligations.

Data intermediaries are also bound by the PDPA and must ensure that they comply with the applicable PDPA obligations set out at **3.1 Objectives and Scope of Data Regulation**.

Action items for organisations therefore include, but are not limited to:

- appointing a responsible officer (ie, DPO);
- monitoring data flows; and
- ensuring contractual compliance with data intermediaries.

3.4 Regulators and Enforcement

See **1.7 Regulators**.

4. Sectoral Topics

4.1 Use of Cookies

In Singapore, there are no standalone statutory rules that specifically regulate cookies, SDKs or similar tracking technologies. Instead, the PDPA applies where these tools are used to collect, use or disclose personal data. The PDPC has clarified that tracking technologies which process personal data are subject to the same requirements as other forms of personal data processing, while cookies that do not identify individuals generally fall outside the PDPA's scope.

A consent-based framework applies according to the Advisory Guidelines for Selected Topics (revised 23 May 2024). For online functions that a user has expressly requested, organisations may not need to obtain separate consent for the use of cookies where the user understands the purpose and voluntarily provides their data. Where a service cannot operate without cookies that process personal data, consent may be deemed if it is reasonable to expect the individual to provide such data for that activity. This includes activities such as:

- authentication and security;
- user preference;
- network management; and
- streaming content.

However, a user's failure to adjust browser or device settings does not, by itself, amount to consent. In contrast, tracking for purposes such as personalised advertising or profiling generally requires clear and express consent, rather than reliance on implied consent or opt-out models.

4.2 Personalised Advertising and Other Online Marketing Practices

Singapore law does not specifically label or regulate “personalised” or “targeted” advertising as a distinct category. Instead, such practices are governed through the PDPA to the extent they involve the collection, use or disclosure of personal data. Where advertising activities rely on profiling or behavioural analysis that identifies or relates to an individual, organisations are generally required to obtain clear and affirmative opt-in consent.

Where marketing involves sensitive personal data and children’s data, see **1.3 Special Categories of Personal Data** for additional constraints that apply.

4.3 Employment Privacy Law

Under Section 4 (1)(a) and (b) of the PDPA, the Data Protection Provisions do not apply to an employee acting in the course of their employment. However, employers remain subject to the PDPA when collecting, using or disclosing personal data about employees, job applicants and former employees.

Generally, employers are required to notify individuals of the purposes for which their personal data is processed and to obtain consent, unless an exception under the PDPA applies. In practice, employers often rely on deemed consent under Sections 15 and 15A of the PDPA, or on specific statutory exceptions set out in Section 17 and the First and Second Schedules to the PDPA.

Where a job applicant voluntarily provides personal data in the course of a job application, consent is typically deemed for the collection, use and disclosure of that data for purposes reasonably related to evaluating the application. If the applicant is subsequently employed, it would generally be reasonable for the employer to continue using the data for employment-related purposes. Where the employer intends to use the data for purposes outside the scope of deemed consent or any applicable exception, fresh consent must be obtained.

The First and Second Schedules to the PDPA permit the processing of employee personal data without

consent in various employment-related scenarios, including:

- assessing an individual’s suitability, eligibility or qualifications for employment, advancement or continued employment; and
- entering into, managing or terminating their employment relationships, or appointment would not require the consent of their employees.

Note that employers are nevertheless required to notify their employees of purposes of such collection, use or disclosure, by providing the individual with the purpose of processing. Upon request, the employer must provide contact details for a person able to address queries relating to the processing.

In remote working arrangements and bring-your-own-device environments, employers may process personal data to safeguard business systems, manage cybersecurity risks and ensure compliance with internal policies. Such processing may be carried out without consent under the “legitimate interests” exception, subject to the notification obligation and other PDPA requirements.

4.4 Data Protection in M&A

In Singapore, the PDPA permits the collection, use and disclosure of personal data without consent in mergers, acquisitions and asset deals, provided the statutory conditions under Part 4 of the First Schedule to the PDPA are satisfied.

The exception covers transactions where an organisation (X) is a party or a prospective party to a business asset transaction with another organisation (Y), and personal data about an applicable individual of Y:

- is collected from Y by X for the purposes of the business asset transaction;
- is used or disclosed by X in relation to the business asset transaction; or
- is disclosed by Y to X for the purposes of the business transaction.

Where the transaction concerns any part of Y or Y’s business assets, the aforementioned personal data transferred must relate directly to that part.

Due Diligence Stage

Where X is only a prospective party to the transaction, it may collect personal data, and Y may disclose such data, only to the extent necessary to determine whether to proceed with the transaction. In addition, the parties must have entered into an agreement requiring X to use or disclose the personal data solely for purposes connected with the transaction.

Post-Completion Use and Notification

If the transaction proceeds, X may use or disclose the personal data collected only for the same purposes for which Y would have been permitted to do so. Any personal data that does not relate directly to the business or assets acquired must be returned or destroyed. The parties must also notify the affected individuals that the transaction has taken place and that their personal data has been disclosed to X.

Incomplete Transactions

If the transaction does not proceed or is not completed, all personal data collected in connection with the transaction must be returned to Y or securely destroyed.

Change-of-Control and Indirect Transactions

Similar rules apply where the transaction involves the transfer of an interest in a third organisation, such as a share sale.

5. International Considerations

5.1 Restrictions on International Data Transfers

In Singapore, the PDPA regulates cross-border personal data transfers. Non-personal data is generally not subject to transfer restrictions unless sector-specific or cybersecurity laws apply. While a “transfer” is not expressly defined in the PDPA, it would broadly cover any disclosure, sending or making available of personal data to a recipient outside Singapore, whether directly or through remote access.

Pursuant to Section 26 of the PDPA, organisations may only transfer personal data overseas if they have taken reasonable steps to ensure that the recipient is subject to binding obligations that afford a level of

protection comparable to the PDPA. Under the PDP Regulations, such obligations may arise from:

- any law;
- any contract requiring the overseas recipient to afford the transferred personal data a level of protection comparable to that under the PDPA, and which identifies the countries and territories to which the personal data may be transferred under the contract;
- any binding corporate rules (in cases where a recipient is an organisation related to the transferring organisation) that require every recipient to provide to the transferred personal data a standard of protection that is at least comparable to the protection under the PDPA, and which specify:
 - (a) the recipients of the transferred personal data to which the binding corporate rules apply;
 - (b) the countries and territories to which the personal data may be transferred under the binding corporate rules; and
 - (c) the rights and obligations provided by the binding corporate rules; or
- any other legally binding instrument.

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

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

The PDP Regulations expressly recognise certification under the APEC Cross-Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP) frameworks as an accepted basis for international data transfers. Where an overseas recipient holds a relevant CBPR or PRP certification that is recognised in its jurisdiction, it is deemed to be subject to enforceable obligations ensuring that the transferred personal data is protected to a standard comparable to that required under the PDPA.

5.2 Government Notifications and Approvals

Singapore does not impose any registration, filing, notification or prior approval requirements with regulatory authorities solely for the purpose of transferring data overseas.

5.3 Data Localisation Requirements

Singapore does not impose explicit data localisation or data residency requirements under the PDPA. Organisations are therefore not obliged to retain personal data, or copies of such data, physically within Singapore, even where the data is stored or processed abroad.

Remote access to personal data from outside Singapore is treated in practice as a form of cross-border transfer. It is permitted so long as the organisation complies with the PDPA's transfer limitation obligation, including taking steps to ensure that overseas recipients or access arrangements afford a level of protection comparable to that required under Singapore law.

5.4 Blocking Statutes

Singapore does not maintain a general "blocking statute" or foreign-judgment control regime that restricts compliance with foreign discovery orders or sanctions. Nevertheless, cross-border disclosures of data are constrained by existing confidentiality and data protection laws. In particular, Section 26 of the PDPA limits the transfer of personal data outside Singapore unless the transferring organisation ensures that the recipient is subject to legally enforceable safeguards providing a level of protection comparable to the PDPA.

Separately, disclosures may be prohibited under the Official Secrets Act and the Statutory Bodies and Government Companies (Protection of Secrecy) Act 1983, which prevents the disclosure of official government-related documents and information.

5.5 Recent Developments

In June 2025, the Global Cross-Border Privacy Rules (CBPR) Forum formally launched the Global CBPR and Privacy Recognition for Processors certification systems, marking a significant development in the facilitation of international personal data transfers.

- The Global CBPR framework establishes a single certification that organisations can rely on to transfer personal data across all participating economies, which currently include Singapore, the United States, Japan, Australia, Canada and several other jurisdictions. Certification is obtained through accredited Accountability Agents, with the IMDA acting as the designated authority in Singapore.
- In Singapore, Global CBPR certification is recognised under the PDPA as a lawful mechanism for overseas data transfers, reducing the need for organisations to implement additional contractual or organisational safeguards when transferring personal data to other member economies.
- Looking ahead, the Global CBPR Forum has signalled plans to expand membership beyond the current group of economies, continuing to build its network of certified organisations – developments that are expected to further shape Singapore's approach to cross-border data transfer compliance.

Trends and Developments

Contributed by:

Chong Kin Lim, David N. Alfred and Anastasia Chen
Drew & Napier LLC

Drew & Napier LLC established a dedicated Data Protection, Privacy and Cybersecurity Practice to leverage its unrivalled experience in data privacy and data and cyber governance and offer clients best-in-class solutions to address their legal and compliance needs in Singapore and across the region. The firm represents many regional companies, multinationals, industry associations, government bodies and regulators, and regularly assists them on a wide range of matters in Singapore and ASEAN member countries.

At the forefront of data protection law in Singapore since 2013, the Data Protection, Privacy & Cybersecurity Practice Group has worked on significant data protection enforcement cases and appeals, including those involving cybersecurity elements. Building on its experience in this field, the Drew Data Protection & Cybersecurity Academy was established in 2020 to offer clients services relating to data protection and cybersecurity compliance, including training, consulting and external data protection officer services.

Authors



Chong Kin Lim heads Drew & Napier's highly regarded TMT practice group. His clients include telecoms and media regulators, global carriers, technology market leaders, global broadcasters and content providers.

Chong Kin has worked on every significant development in the Singapore TMT market, and continues to play a key role in the development of sectoral competition regulation in Singapore. He was the lead external counsel in the liberalisation of the telecommunications, media and postal sectors, and has assisted regulators in conceptualising and drafting "first-of-its-kind" sectoral competition legislation and frameworks.



David N. Alfred is a director of Drew & Napier LLC and co-head of the firm's Data Protection, Privacy & Cybersecurity Practice Group. He is concurrently co-head and programme director of the Drew Data Protection &

Cybersecurity Academy. David is a data protection, cybersecurity and technology lawyer with over 25 years' experience advising on a broad range of matters relating to digital technology,

telecommunications and the internet. He has substantial experience advising on data protection and cybersecurity compliance, regulatory enforcement, data breaches and international aspects of data protection. Prior to joining the firm, David was the first Chief Counsel of Singapore's data protection authority, the Personal Data Protection Commission.



Anastasia Chen is a director of Drew & Napier LLC and deputy head of the firm's Data Protection, Privacy & Cybersecurity Practice Group. Prior to joining the firm, Anastasia was Deputy Chief Counsel to Singapore's

Personal Data Protection Commission (PDPC) and Info-communications Media Development Authority (IMDA) for over nine years, during which she served as lead counsel for PDPC's matters, IMDA's procurement and intellectual property portfolios, as well as IMDA's Data Administration Group. She has received accolades from legal publications, with clients commending her deep industry and regulatory expertise, as well as legal acumen, especially when dealing with novel problems.

Drew & Napier LLC

10 Collyer Quay
10th Floor
Ocean Financial Centre
Singapore 049315

Tel: +65 6531 4110
Fax: +65 6535 4864
Email: mail@drewnapier.com
Web: www.drewnapier.com



Introduction

Businesses in Singapore are increasingly confronted with the challenge of staying compliant and secure with data protection regulations, in the face of rapid adoption of digital services, increased data sharing, and AI risks. That said, the Personal Data Protection Commission (PDPC) remains cognisant and responsive, refining, administering and enforcing Singapore's Personal Data Protection Act (PDPA) in ways that support and balance accountability and innovation.

This chapter of the guide unpacks the following topics which have recently taken on increasing relevance:

- cross-border data transfers;
- protection of data in the context of AI deployment;
- phasing out of National Registration Identity Card (NRIC) numbers for authentication;
- amendments to the Public Sector (Governance) Act (PSGA); and
- local enforcement trends.

Cross-Border Data Transfers

Cross-border data transfers remain central to Singapore's digital economy, supporting e-commerce and other digitally enabled functions such as data analytics and AI deployment. As organisations increasingly rely on global technology vendors and distributed data infrastructures, compliance with cross-border transfer rules continues to be both an operational necessity and a strategic consideration.

Cross-border data transfers are governed by Section 26 of the PDPA, which provides that organisations must ensure that any overseas recipient provides a

standard of protection to the transferred personal data that is at least comparable to the PDPA. In practice, this is typically achieved through contractual safeguards.

EU-Singapore Digital Trade Agreement (EUSDTA)

A recent development in this area is the entry into force of the EUSDTA on 1 February 2026. As a key digital trade partner of the European Union, Singapore's entry into the EUSDTA reflects both parties' commitment to open, rules-based digital trade, while upholding strong protections for personal data and privacy in cross-border digital transactions.

The EUSDTA introduces binding commitments designed to facilitate cross-border digital transactions and reduce regulatory uncertainty. These include provisions to:

- strengthen online consumer protection;
- protect personal data and privacy;
- promote paperless trade;
- recognise electronic signatures and contracts; and
- prohibit unjustified data localisation requirements or forced transfers of source code.

The EUSDTA is particularly relevant for businesses operating between Singapore and the EU that rely on cloud-based platforms, cross-border analytics or regional technology providers. While the EUSDTA does not replace domestic data protection obligations, it signals a continued policy direction towards enabling trusted data flows through interoperable digital trade rules.

Contractual and certification mechanisms

The PDPC continues to recognise a range of practical mechanisms to facilitate cross-border transfers that are compliant with the PDPA's transfer limitation obligation.

At a regional level, the ASEAN Model Contractual Clauses are recognised and encouraged by the PDPC as a practical contractual mechanism, particularly for organisations with intra-group or vendor-related transfers within South-East Asia. These standardised clauses are designed to align with the ASEAN Framework on Personal Data Protection 2016 and can help streamline negotiations across multiple ASEAN jurisdictions.

In addition, Regulation 12 of the Personal Data Protection Regulations 2021 recognises certifications under the APEC Cross-Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP) systems as mechanisms that satisfy the transfer limitation obligation. These certifications provide a structured, internationally recognised approach to demonstrating comparable data protection standards across participating economies.

Building on the aforementioned cross-border privacy mechanisms, the Global CBPR and Global PRP systems were introduced in June 2025 as broader international certification frameworks. While Singapore's regulations currently recognise only the APEC CBPR and PRP certifications, the Global CBPR framework reflects a wider trend towards interoperable, certification-based transfer regimes.

Taken together, these developments point to an increasingly layered cross-border data governance environment. Businesses operating across multiple jurisdictions should therefore consider both treaty-level developments, such as the EU-Singapore DTA, and practical compliance tools, such as contractual clauses and recognised certifications, when structuring their data transfer arrangements.

Data Protection in the Context of AI Deployment

Singapore introduced three new initiatives in July 2025:

- the new Global AI Assurance Sandbox;
- a new privacy enhancing technology (PET) adoption guide; and
- the Singapore Standard for Data Protection.

The Global AI Assurance Sandbox

The Global AI Assurance Sandbox aims to provide a conducive environment for organisations to trial responsible AI applications, offering tools, resources and a controlled setting for practical testing. Building on insights from an earlier pilot phase, the sandbox now covers additional AI archetypes, such as agentic AI, as well as emerging risks including data leakage and prompt injection vulnerabilities. It addresses a broad range of AI-related risks and is also relevant from a data protection perspective, as it enables organisations to assess how their AI systems manage data-related risks before full-scale deployment. The sandbox may also be opened to sectoral regulators to test governance or assurance approaches, with insights feeding into future policy guidance and potential accreditation frameworks for AI testers.

PETs Adoption Guide

PETs protect personal data while allowing organisations to use such data for AI development and training and are increasingly positioned as practical tools to enable data-driven innovation without compromising privacy. First introduced in 2022 by the IMDA and PDPC, Singapore's PET Sandbox now explores how PETs can be applied to generative AI use cases while managing associated data protection risks. Drawing on insights from these sandbox projects, IMDA has released a new PETs Adoption Guide to help organisations deploy PETs and derive greater value from their data. The guide includes a "PETs Use Case Evaluation Tool" to assist organisations in identifying suitable PET solutions, as well as an "Implementation Checklist" to support the end-to-end adoption process. IMDA has emphasised that the guide is intended to be a "living document", with ongoing refinements based on industry feedback and additional use cases.

The Singapore Standard for Data Protection

The Data Protection Trustmark was elevated into a new Singapore Standard (SS 714:2025), aligning it with international data protection benchmarks and best practices. Organisations can now apply for certi-

fication under this enhanced framework, which serves as a recognised mark of accountable data protection practices and provides assurance to consumers and regulators on the organisation's handling of personal data. The new standard introduces clearer requirements in areas such as third-party management and overseas data transfers and is overseen by the Singapore Accreditation Council to ensure certification assessments meet globally recognised standards. For organisations, certification under the Singapore Standard serves as an externally recognised indicator of robust and accountable data governance.

For businesses deploying AI systems, the developments signal increasing regulatory expectations around testing, assurance and accountable data practices. Organisations should consider whether PETs can be incorporated into AI development pipelines, assess participation in regulatory sandboxes where appropriate, and evaluate certification frameworks such as the Data Protection Trustmark as part of their broader AI and data governance strategies.

Phasing Out of NRIC Numbers for Authentication

In February 2026, the PDPC announced that private organisations must cease using NRIC numbers for authentication purposes by 31 December 2026. Organisations that continue to rely on full or partial NRIC numbers as authentication credentials may be found to have breached Section 24 of the PDPA for failing to implement reasonable security arrangements, with enforcement expected to intensify from 1 January 2027.

This development builds on the June 2025 joint advisory issued by the PDPC and the Cyber Security Agency of Singapore, which clarified that NRIC numbers should not be used as authentication credentials. Practices such as using NRIC numbers as default passwords, or combining them with easily obtainable information like names or dates of birth, have been identified as insecure because NRIC numbers are widely used identifiers and may be readily exposed or guessed.

For businesses, the announcement may require significant changes to existing systems and processes. Many organisations, particularly in sectors such as tel-

ecomunications, healthcare and financial services, have historically relied on NRIC-based verification for user portals and access to digital documents. These organisations will need to review their existing authentication workflows and implement more secure alternatives, such as one-time passwords, authenticator applications or multi-factor authentication.

More broadly, the phase-out reflects the PDPC's continued emphasis on security-by-design and the expectation that authentication methods should be proportionate to the sensitivity of the personal data involved. Organisations with legacy systems or large customer bases should therefore prioritise transition planning well ahead of the 31 December 2026 deadline.

Amendments to the PSGA

In January 2026, Parliament passed amendments to the PSGA, marking a notable development in Singapore's public-sector data governance framework. The amendments are intended to streamline data-sharing processes to support the more efficient delivery of public services, including by extending the data-sharing regime to trusted external partners beyond the public sector engaged by the government.

The amendments permit public agencies to share data with such trusted external partners, provided that the sharing serves the same seven public-interest purposes recognised under the Act. This represents a measured expansion of the original framework, which previously focused on data sharing among public agencies. The change reflects the practical reality that many public services are delivered in collaboration with external organisations, such as social service providers, research institutions, and private-sector vendors, which may require access to government-held data to perform their functions effectively.

To address the risks associated with extending data access beyond the public sector, the amendments introduce three key safeguards for data sharing with external partners:

- data may only be shared where it serves one of the legitimate public-interest purposes specified under the PSGA;

- the sharing arrangement must be authorised by the relevant Minister or a delegated authority, with the approval specifying the purpose of the sharing, the scope of data involved, and the external partners permitted to receive it; and
- external partners must be subject to contractually binding terms of use that impose data protection and security requirements at least equivalent to those applicable to public agencies.

Individuals working for such partners may also face criminal liability for misuse of shared data, with penalties aligned to those applicable to public officers under the PSGA.

The amendments also clarify that public agencies may use, and not merely share, data for the purposes specified under the PSGA, while remaining subject to existing internal governance and security requirements. Importantly, the PSGA does not override confidentiality obligations imposed under other written laws, legal privilege or contractual arrangements.

For the private sector, the amendments are particularly relevant to organisations that provide services to, or partner with, government agencies. External partners, such as technology vendors, data analytics providers and contractors, may now receive government-held data under a statutory framework, leading to more structured arrangements with public-sector-aligned data protection, security and accountability requirements. Furthermore, these external partners should expect heightened scrutiny of their data governance practices and be prepared to meet public-sector standards of accountability and security.

Enforcement Trends

The PDPC has been taking a strong enforcement stance against breaches of the various obligations under the PDPA. In *Re Marina Bay Sands Pte Ltd [2025] SGPDP 6*, the PDPC meted out its second largest financial penalty (to date) of SGD315,000, having factored in the annual turnover of the organisation in determining the financial penalty amount.

Clarity on financial penalty framework

From 1 October 2022, Parliament raised the maximum financial penalty for large organisations with annual

turnovers in Singapore over SGD10 million, to 10% of their annual turnovers.

The PDPC has now, for the first time, in *Re Marina Bay Sands Pte Ltd [2025] SGPDP 6*, articulated key aspects of its financial penalty framework for determining the quantum of financial penalties under the PDPA.

In brief, Marina Bay Sands (MBS) is an integrated resort operator that runs, among other things, two membership programmes: Sands Rewards Lifestyle and ArtScience Friend. In October 2023, the personal data of 665,495 MBS patrons was illegally accessed and exfiltrated by unknown actors. The affected data, including names and contact details that identified MBS's patrons, was later found for sale on the dark web. MBS admitted to breaching the protection obligation, by failing to take reasonable security measures to protect the personal data in its possession.

The PDPC's financial penalty framework is subject to the following guiding principles.

- The framework aims to effectively deter non-compliance with the PDPA, while ensuring proportionality to the seriousness of the non-compliance.
- When considering the relative weight to be given to effective deterrence and proportionality, consideration has to be given to the PDPA's overarching balance of the right of individuals to protect their personal data and organisations' need to process personal data for legitimate purposes.
- There should be like and consistent treatment in the two-tiered financial penalty regime for organisations with annual turnovers of SGD10 million and below, and organisations with annual turnovers above SGD10 million. Annual turnover size should be accorded more weight for organisations with annual turnovers above SGD10 million. Other relevant factors must be given similar weight in like cases.
- The financial penalty framework must be applied in a fact-sensitive manner.

With these in mind, the Penalty Framework comprises the following steps.

- *Preliminary step* – The PDPC first identifies the applicable statutory maximum financial penalty under Section 48J(3) of the PDPA. It then determines an appropriate percentage rate or quantum cap, not exceeding that statutory maximum, based on the nature of the contravention. In general, intentional breaches attract higher rates than negligent ones, and this exercise establishes the maximum financial penalty applicable for the case before the subsequent steps of the framework are applied.
 - *A five-step methodology* then applies.
 - (a) Step 1 – Identification of level of culpability and harm. The PDPC assesses all relevant factors, including the nature, gravity and duration of the non-compliance, to determine the organisation’s level of culpability as “low”, “medium” or “high”. It will also assess whether the level of harm is “slight”, “moderate” or “severe”, taking into account factors such as the type and sensitivity of the affected data, the number of individuals impacted, and the extent of actual or potential harm.
 - (b) Step 2 – Calculation of the starting financial penalty. Based on the assessed levels of culpability and harm in Step 1, the PDPC identifies the corresponding starting range and determines an appropriate starting financial penalty within that range.
 - (c) Step 3 – Adjustment for aggravating and mitigating factors. The PDPC then adjusts the starting financial penalty identified in Step 2 to reflect relevant aggravating and mitigating considerations, such as the organisation’s cooperation, remedial actions, prior compliance record or any benefit derived from the contravention.
 - (d) Step 4 – The PDPC considers whether the proposed financial penalty would adversely affect the organisation’s ability to continue its usual operations, based on the available evidence. Where appropriate, it may extend the payment timeline, allow instalment payments or reduce the penalty amount.
 - (e) Step 5 – Final adjustments. The PDPC conducts a final review of the quantum to ensure that the resulting financial penalty is both effective as a deterrent and proportionate in the circumstances of the case.
- Applying this framework, the PDPC found that the maximum financial penalty applicable to MBS was 10% of its turnover. Applying Step 1, MBS’s level of culpability was low, but there was a moderate level of harm due to the large number of affected individuals. The PDPC then determined the starting financial penalty within the low-moderate band and adjusted this to account for relevant mitigating factors, including MBS’s voluntary notification to affected individuals and prompt remedial measures. This ultimately resulted in a reduced financial penalty of SGD315,000, which the PDPC found would not adversely affect MBS’s ability to carry out its usual operations.
- The decision signals the PDPC’s increasing emphasis on deterrence, as substantial penalties may be imposed even where the compromised data is not highly sensitive. It also underscores the regulator’s expectations that organisations implement robust operational controls, rather than relying solely on individual employees, particularly where large volumes of personal data are involved. Businesses should place increased emphasis on data protection and cybersecurity.

Conclusion

Singapore’s data protection landscape is evolving alongside developments in digital trade, AI and data-driven public services, with a clear emphasis on enabling innovation while strengthening accountability and security obligations.

For businesses, compliance should not be treated as a static or one-off exercise. Recent developments across digital services, AI governance, authentication practices and public-sector data sharing, coupled with increased enforcement scrutiny, point to a more integrated, risk-based data environment.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Rob.Thomson@chambers.com