GDR

INSIGHT HANDBOOK
2024

The GDR *Insight Handbook 2024* delivers specialist intelligence and research to our readers – general counsel, government agencies and private practitioners – who must navigate the world's increasingly complex framework of data legislation. In preparing this report, Global Data Review has worked with leading data lawyers and consultancy experts from around the world.

Visit globaldatareview.com
Follow @GDR_alerts on Twitter
Find us on LinkedIn

Singapore: EU Cooperation and AI Governance Testing Keep City State at the Cutting Edge

Lim Chong Kin and Anastasia Su-Anne Chen
Drew & Napier LLC

Key statutes, regulations and adopted international standards

The Personal Data Protection Act 2012 (PDPA) is the key data protection legislation in Singapore. It governs the collection, use and disclosure of individuals' personal data by all private sector organisations.

The PDPA comprises two main parts: Parts 3 to 6A (the Data Protection Provisions) set out the general obligations of organisations with regard to their management of personal data, while Part 9 of the PDPA (the DNC Provisions) contains provisions establishing the Do Not Call (DNC) Registry and obligations of organisations that send marketing messages to Singapore telephone numbers.

Several regulations have been issued under the PDPA, including:

- the Personal Data Protection (PDP) Regulations 2021;
- the Personal Data Protection (Notification of Data Breaches) Regulations 2021;
- the Personal Data Protection (Composition of Offences) Regulations 2021;
- the Personal Data Protection (Do Not Call Registry) Regulations 2013;
- the Personal Data Protection (Enforcement) Regulations 2021; and
- the Personal Data Protection (Appeal) Regulations 2021.

The Singapore data protection authority, the Personal Data Protection Commission (PDPC), has issued a number of advisory guidelines detailing how it will interpret the provisions of the PDPA. These range from general guidelines on key concepts in the PDPA and selected topics, to sector-specific advisory guidelines for sectors such as the telecommunications, real estate, education, healthcare and social services and insurance.

The PDPA was amended under the Personal Data Protection (Amendment) Act 2020 (the Amendment Act) on 2 November 2020. Most of the amendments have come into force. For example, the expansion of the consent obligation, the introduction of a mandatory data breach notification regime and the introduction of criminal penalties for the egregious misuse of personal data, came into force on 1 February 2021. As of 1 October 2022, the financial penalty cap for breaches under the PDPA has increased from S$1 million to S$1 million or 10 per cent of the organisation's annual turnover in Singapore, whichever is higher; however, the new data portability obligation will only come into force at a later date.

Aside from the PDPA, a number of other pieces of legislation and regulatory instruments in Singapore contain sector-specific data protection requirements. For example:

- in the financial sector, provisions governing customer information obtained by banks are set out in the Banking Act 1970. The Monetary Authority of Singapore (MAS) issues directives and notices concerning data protection for the financial sector, such as the Notices and Guidelines on Technology Risk Management, the Notices on Cyber Hygiene and the Guidelines on Outsourcing;
- in the healthcare sector, confidentiality of medical information and the retention of medical records are governed by the Private Hospitals and Medical Clinics Act 1980 and the Healthcare Services Act 2020; and
- in the telecommunications sector, the Code of Practice for Competition in the Provision of Telecommunication and Media Services 2022 issued under the Telecommunications Act 1999 regulates the telecommunications licensees' use of end-user service information.

Other legislation that may have an indirect impact on data protection includes:

- the Computer Misuse Act 1993, which contains offences for the unauthorised access or modification of computer material and the unauthorised use or interception of computer services; and
- the Cybersecurity Act 2018, which requires owners and operators of critical information infrastructure to comply with cybersecurity codes of practices and standards of performance, conduct regular audits and risk assessments, and report on cybersecurity incidents.

The rights or obligations under specific legislation are not affected by the general data protection framework under the PDPA. As provided under section 4(6) of the PDPA, in the event of any inconsistency, the provisions of the other specific legislation will prevail.

Adopted international standards

Singapore participates in the Cross-Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP) systems of the Asia-Pacific Economic Cooperation (APEC). The APEC CBPR and PRP are multilateral certification schemes that allow participating businesses and other organisations to develop their own internal rules and policies consistent with the specific CBPR and PRP programme requirements to facilitate cross-border data transfers across the participating economies.

On 1 June 2020, the PDP Regulations 2014, which have since been superseded by the PDP Regulations 2021, were amended to recognise the APEC CBPR system and PRP system certifications for overseas transfers of personal data under the PDPA.

Regulatory bodies

The PDPA establishes the PDPC, which is the data protection authority responsible for administering and enforcing the PDPA. The PDPC is under the purview of the telecommunications and media regulator, the Infocomm Media Development Authority (IMDA). Sectoral regulators separately enforce the data protection obligations within their relevant sectors.

The PDPC may give any direction to the organisation to ensure compliance with the PDPA, for example, a direction to:

- stop collecting, using or disclosing personal data in contravention of the PDPA; or
- destroy personal data collected in contravention of the PDPA.[1]

Further, if the PDPC is satisfied that the organisation intentionally or negligently contravened the PDPA, it may require the organisation to pay a financial penalty not exceeding S$1 million or 10 per cent of the organisation's annual turnover in Singapore, whichever is higher.

In carrying out its investigative functions, the PDPC is empowered to:

- require any organisation to produce any specified document or information;
- enter an organisation's premises without a warrant; and
- obtain a search warrant to enter an organisation's premises and search the premises or any person on the premises, and take possession of, or remove, any document and equipment or article relevant to an investigation.[2]

1 Personal Data Protection Act 2012 (PDPA), section 48I(2).
2 PDPA, section 50(2) read with the Ninth Schedule.

The changes under the Amendment Act strengthen the PDPC's enforcement powers by providing additional recourse to compel attendance of witnesses, the provision of information, and the production of documents. Criminal sanctions may also be imposed on individuals and organisations for obstructing or hindering the investigations of the PDPC or providing any false or misleading statements or information to the PDPC.[3] In particular, individuals may be liable to a fine of up to S$10,000 and imprisonment for a term of up to 12 months, or both, while organisations may be liable to a fine of up to S$100,000.

The PDPC also has the power to:

- discontinue investigations and simply issue an advisory notice where the impact is assessed to be low;
- initiate an undertaking process, which includes a written agreement between the organisation and the PDPC in which the organisation voluntarily commits to remedy the breaches and take steps to prevent recurrence; and
- issue an expedited breach decision in certain circumstances where there is an upfront, voluntary admission of liability for breaching the PDPA.

The PDPC has been active in its enforcement of the PDPA. As at 30 June 2023, the PDPC had issued a total of 236 decisions, with a significant majority relating to breaches of the protection obligation. Of those decisions, some of the most common breaches of the PDPA have arisen from inadequate technical security arrangements, human error, technical faults and insufficient data protection policies.

The effect of local laws on foreign businesses

Subject to its detailed scope, the PDPA applies to all organisations that are not public agencies. In particular, it defines 'organisation' broadly to mean 'any individual, company, association or body of persons, corporate or unincorporated, whether or not – (a) formed or recognised under the law of Singapore; or (b) resident, or having an office or a place of business, in Singapore'.[4] As such, the applicability of the PDPA can extend to foreign businesses.

The PDPC has indicated in its Advisory Guidelines on Key Concepts in the PDPA that its interpretation of the extraterritorial scope of the PDPA is that the 'Data Protection Provisions [under the PDPA] apply to organisations carrying out activities involving personal data in Singapore';[5] therefore, an organisation, including a foreign company, would have to ensure compliance with the PDPA in respect of its activities involving personal data in Singapore, namely the

3 PDPA, section 51.
4 PDPA, section 2.
5 Advisory Guidelines on Key Concepts in the PDPA, section 11.1.

collection, use, disclosure or other processing of personal data in Singapore. This could extend to foreign companies collecting personal data of individuals based in Singapore or the hosting of personal data in Singapore (which originated overseas).

In *Re Cigna Europe Insurance Company SA-NV*,[6] the PDPC investigated a Belgium-based company, which was offering health insurance solutions and coverage in Singapore through a registered branch office, for two data breach incidents in 2017 and 2018. Nevertheless, on the facts, the PDPC found that the organisation was in compliance with the PDPA.

Core principles on personal data

Definition of personal data

'Personal data' is broadly defined under the PDPA as 'means data, whether true or not, about an individual who can be identified – (a) from that data; or (b) from that data and other information to which the organisation has or is likely to have access'.[7]

While the PDPA does not have a specific definition of 'sensitive personal data', the PDPC has taken the position in several enforcement decisions that a higher standard of protection is required for personal data that is more sensitive in nature. These types of personal data include National Registration Identification Card numbers, insurance data, medical data, financial data and children's data.[8]

Data protection obligations

The Data Protection Provisions contain, at present, 10 main obligations that organisations are required to comply with if they undertake activities relating to the collection, use or disclosure of personal data. There is another data protection obligation – the data portability obligation – that is not currently in force, but will come into force at a later date.

6 *Re Cigna Europe Insurance Company SA-NV* [2019] SGPDPC 18.
7 PDPA, section 2.
8 *Re Aviva Ltd* [2017] SGPDPC 14; *Re Credit Counselling Singapore* [2017] SGPDPC 18; *Re Singapore Taekwondo Federation* [2018] SGPDPC 17; *Re AIA Singapore Private Limited* [2019] SGPDPC 20.

Consent obligation

An organisation must obtain the consent of an individual before collecting, using or disclosing their personal data for a purpose, unless an exception in the First or Second Schedule to the PDPA applies.[9] Some examples of exceptions to consent include where the personal data is publicly available; or the collection, use or disclosure is necessary to respond to an emergency that threatens the life, health or safety of the individual. The Amendment Act introduced two new exceptions to the consent requirement: the 'legitimate interests'[10] and 'business improvement'[11] exceptions.

For consent to be considered validly given, the organisation must first inform the individual of the purposes for which their personal data will be collected, used or disclosed. These purposes have to be what a reasonable person would consider appropriate in the circumstances. Fresh consent must be obtained where personal data is to be used for any new purpose that the individual has not consented to (unless there is an applicable exception).

Consent may also be deemed to have been given where an individual has voluntarily provided their data to an organisation for a purpose, and it is reasonable that the individual does so.[12] The onus is on the organisation to establish that the individual was aware of the purposes for which the personal data was provided. The concept of deemed consent under the PDPA has also recently been expanded to include deemed consent by contractual necessity[13] and deemed consent by notification.[14]

Consent obtained in the following ways does not constitute valid consent for the purpose of the PDPA:

- where consent is obtained as a condition of providing a product or service, and the consent is beyond what is reasonable to provide the product or service to the individual; and

9 PDPA, section 13.

10 The 'legitimate interests' exception enables organisations to collect, use or disclose personal data without consent in circumstances where there is a need to protect the lawful Interests of the organisation or any other person. Organisations wishing to rely on this legitimate interests basis must fulfil certain requirements (eg, conducting a risk and impact assessment).

11 The 'business improvement' exception provides that organisations can use personal data for the purposes of operational efficiency and service improvements; product and service development; or knowing customers better, subject to the fulfilment of certain requirements.

12 PDPA, section 15.

13 For deemed consent by contractual necessity, consent is deemed to have been given for the disclosure of personal data where it is reasonably necessary for the conclusion or performance of a contract or transaction between the individual and the organisation.

14 For deemed consent by notification, subject to fulfilling certain conditions, consent is deemed to have been given if the organisation provides appropriate notification as to the purpose of such processing, with a reasonable period for the individual to opt out; and the individual did not opt out within the period.

- where false or misleading information is provided, or deceptive or misleading practices are used, to obtain or attempt to obtain the individual's consent for collecting, using or disclosing personal data.[15]

Individuals may also withdraw any consent given or deemed to have been given at any time by giving reasonable notice to the organisation.[16]

Notification obligation

Organisations are obliged to inform individuals of the purposes for the collection, use or disclosure of their personal data, on or before collecting the personal data; and any other purpose for the use or disclosure of personal data that has not been notified to the individual, before such use or disclosure of personal data. The PDPA does not prescribe the manner or form in which individuals have to be notified.

Purpose limitation obligation

An organisation may collect, use or disclose personal data about an individual only for purposes that a reasonable person would consider appropriate in the circumstances and, if applicable, have been notified to the individual concerned.[17]

Access and correction obligations

Under the access obligation, an organisation must allow an individual to access their personal data in its possession or under its control upon request as soon as reasonably possible, subject to the exceptions in section 21(3) of the PDPA and in the Fifth Schedule to the PDPA.[18] The organisation is also obliged to provide the individual with information about the ways in which the personal data may have been used or disclosed during the past year.

Under the correction obligation, individuals have the right to request an organisation to correct any inaccurate data that is in the organisation's control, subject to the exceptions in section 22 of the PDPA and the Sixth Schedule to the PDPA.[19] The organisation, if satisfied on reasonable grounds that a correction must be made, is required to correct the individual's personal data as soon as practicable and send the corrected or updated personal data to specific organisations to which the data was disclosed within a year before the correction was made.

15 PDPA, section 14(2).
16 PDPA, section 16.
17 PDPA, section 18.
18 PDPA, section 21.
19 PDPA, section 22.

The PDP Regulations 2021 set out further details on the access and correction obligations, for example, how an access or correction request may be made, the time frame for providing a response, and whether a fee may be charged for responding to a request.

Accuracy obligation

Organisations must make a reasonable effort to ensure that the personal data they collect is accurate and complete, if 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.[20]

Protection obligation

An organisation must make reasonable security arrangements to protect personal data in its possession or under its control, in order to prevent (1) unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks; and (2) the loss of any storage medium or device on which personal data is stored.[21]

Retention limitation obligation

An organisation must cease to retain documents containing personal data, or remove the means by which the personal data can be associated with particular individuals as soon as it is reasonable to assume that the purpose for which the personal data was collected is no longer being served by retention of the personal data, and the retention is no longer necessary for legal or business purposes.[22]

Transfer limitation obligation

An organisation must not transfer personal data to a country or territory outside Singapore except in accordance with the requirements prescribed under the PDPA and Part 3 of the PDP Regulations 2021 to ensure that the transferred personal data will be accorded a standard of protection that is comparable to that under the PDPA.[23]

20 PDPA, section 23.
21 PDPA, section 24.
22 PDPA, section 25.
23 PDPA, section 26.

In particular, organisations must ensure that the recipients of that personal data are bound by legally enforceable obligations to protect the transferred personal data to a standard that is at least comparable to that under the PDPA. These legally enforceable obligations include obligations imposed under law, contract or binding corporate rules, or any other legally binding instrument.[24]

Data breach notification obligation

An organisation may be required to notify certain data breaches to one or more of the following: affected individuals, the PDPC or the organisation (including a public agency) on whose behalf they are processing personal data when acting as data intermediary.[25]

See the section on 'Data protection breaches' for further detail.[26]

Accountability obligation

Organisations must take responsibility for the personal data in their possession or control and be able to demonstrate that they do so.[27] This includes:

- developing and implementing data protection policies;
- communicating to and informing their staff of those policies;
- implementing processes and practices that are necessary to meet their obligations under the PDPA;
- making information about their data protection policies and practices available to individuals upon request; and
- appointing a data protection officer (DPO) to be responsible for ensuring that the organisation is in compliance with the PDPA.[28]

The PDPC also recommends that organisations conduct a data protection impact assessment (DPIA) to assess whether their handling of personal data is in compliance with the PDPA. A DPIA would involve identifying, assessing and addressing personal data protection risks based on the organisation's functions, needs and processes.

24 Personal Data Protection Regulations 2021, Regulation 11(1).
25 PDPA, sections 26C and 26D.
26 PDPA, sections 26C(3) and 26E.
27 PDPA, section 11. Previously known as the openness obligation.
28 PDPA, section 12.

Data intermediaries

The PDPA makes provision for the processing of personal data by data intermediaries, defined as an organisation that processes personal data on behalf of and for the purposes of another organisation pursuant to a contract that is evidenced or made in writing. Data intermediaries are only subject to the protection and retention limitation obligations, as well as an additional obligation to notify the organisation for which it is processing personal data of a data breach without undue delay.[29] When an organisation employs a data intermediary to process personal data on its behalf and for its purposes, that organisation has the same obligation under the PDPA as if the personal data were processed by the organisation itself.

Automated processing, profiling and data analytics

The PDPC does not have express provisions on automated individual decision-making, data analytics and profiling. If an organisation wishes to carry out automated processing, it will need to ensure that it complies with all generally applicable data protection and privacy laws, such as obtaining necessary consents unless an exception under the PDPA applies.

Communications and marketing

Sending specified messages

The DNC Provisions[30] under the PDPA prohibit organisations from sending specified messages to Singapore telephone numbers registered in the DNC registry. Individuals may choose to opt out of receiving specified messages via voice calls (No Voice Call Register); specified text messages, including any text, sound or visual message, such as SMS, MMS or WhatsApp messages (No Text Message Register); and specified fax messages (No Fax Register).

Subject to certain exceptions, a message constitutes a 'specified message' under section 37 of the PDPA if one of the purposes of the message is:

- to advertise, promote, or offer to supply or provide:
    - goods or services;

29 PDPA, section 4(2).

30 The Amendment Act made certain changes to Part 9 of the PDPA, which includes: inserting a new Part 9A into the PDPA with provisions prohibiting the sending of specified messages to telephone numbers obtained through the use of dictionary attacks and address harvesting software; and imposing an obligation on third-party checkers to communicate accurate Do Not Call registry query results to organisations on whose behalf they are checking the registry.

- land or an interest in land; or
- a business or investment opportunity; or

- to advertise or promote a supplier or provider, or prospective supplier or provider for the above or any other prescribed purpose.[31]

In most instances, a marketing message of a commercial nature sent to an individual would be classified as a specified message under the PDPA.

Under section 43 of the PDPA, an organisation that intends to send a specified message to a user or subscriber of a Singaporean telephone number must check with the relevant DNC register to confirm that the telephone number is not listed in the register, unless the organisation has obtained:

- clear and unambiguous consent from the user or subscriber of the telephone number, evidenced in written or other forms so as to be accessible for subsequent reference; or
- confirmation from a third-party checker that the Singaporean telephone number is not listed in the DNC registry, and the organisation has no reason to believe that, and is not reckless as to whether, among other things, such information is false or inaccurate.

When sending marketing communications to a Singaporean telephone number, organisations must comply with certain requirements, including the following:

- for messages, organisations must include information identifying the sender and how the sender can be readily contacted in the message. Such information has to be reasonably likely to be valid for at least 30 days after the message is sent; and
- for voice calls, not to conceal or withhold the identity of the caller from the recipient.[32]

Certain senders that are in an ongoing relationship with individuals may be excluded from the obligation to check the DNC registry before sending specified text or fax messages related to that relationship.[33] Conversely, one-off transactions are insufficient to establish an ongoing relationship, and organisations may not rely on the ongoing relationship exclusion once it has ceased.

31 PDPA, Tenth Schedule.
32 PDPA, sections 44 and 45.
33 PDPA, paragraph 1(1)(e) of the Eighth Schedule.

SCA

Aside from the DNC Provisions, the Spam Control Act 2007 (SCA) governs the control of spam, namely unsolicited commercial communications sent in bulk by email, instant messages (on platforms such as Telegram and WeChat), SMS or MMS to mobile telephone numbers. The SCA applies as long as the electronic message has a Singapore link.

Under section 11 of the SCA, any sender of unsolicited commercial electronic messages in bulk must comply with the requirements in the Second Schedule to the SCA.

Individuals' rights

Individuals have the right to request an organisation to give them access to or correct the personal data in the organisation's possession or control. In addition, the Amendment Act introduced a new data portability obligation, which will come into force at a later date. Under this new obligation, an individual can require an organisation to transmit personal data to another organisation in a commonly used machine-readable format.

Individuals also have a right to give and withdraw consent at any time by giving reasonable notice; however, this would not affect any legal consequences arising from such withdrawal.[34] Upon withdrawal of consent, the organisation must cease (and cause its data intermediaries and agents to cease) collecting, using or disclosing the personal data, as the case may be, unless the collection, use or disclosure of the personal data without consent is required or authorised under the PDPA or any other written law.

An individual may lodge a complaint against an organisation with the PDPC at any time. Individuals also have a right of private action for loss or damage in respect of an organisation's breach of the PDPA; however, if the PDPC has made a decision under the PDPA in respect of the breach, the private action may only commence after the PDPC's decision has become final (ie, where there is no further right of appeal against the decision).[35]

The role of the DPO

As part of the accountability obligation, it is mandatory for organisations to appoint a DPO.[36] The responsibility of the DPO is to ensure that the organisation complies with the PDPA by developing and implementing policies and processes

34 PDPA, section 16.
35 PDPA, section 480(2).
36 PDPA, section 11(3).

for handling personal data and managing data protection-related queries and complaints, among other things. The DPO also plays an essential role in fostering a data protection culture among employees and communicating personal data protection policies to the various stakeholders; however, the legal responsibility for complying with the PDPA remains with the organisation, rather than the DPO.

Organisations are required to make available the business contact information of its DPO (or any individual to whom the responsibility has been delegated). Similarly, organisations are also required to make available the business contact information of a person who is able to respond to questions relating to the collection, use or disclosure of personal data on behalf of the organisation. This person may also be the DPO.[37]

While there is no requirement that such a person must be located in Singapore, to facilitate prompt responses to queries or complaints, the PDPC recommends that the business contact information of this person should be readily accessible from Singapore, operational during Singapore business hours and provide Singapore telephone numbers (where used).

Data protection breaches

Recent amendments to the PDPA introduced a mandatory data breach notification regime. Under that new regime (Part 6A of the PDPA), in the event of a data breach, organisations are required to conduct, in a reasonable and expeditious manner, an assessment of whether the data breach is a notifiable data breach.

A data breach is a 'notifiable data breach' if it:

- results in, or is likely to result in, significant harm to any individual to whom any personal data affected by a data breach relates; or
- is, or is likely to be, of a significant scale (ie, 500 or more individuals).

The organisation must notify the PDPC of the notifiable data breach as soon as practicable, but in any case, no later than three calendar days after making the determination that a data breach is notifiable. Where a data intermediary has reason to believe that a data breach has occurred in relation to personal data it is processing on behalf of the primary organisation, it must notify the primary organisation without undue delay.

37 PDPA, section 11(5).

Organisations must notify affected individuals if the data breach is likely to result in significant harm.[38] There are two exceptions to this requirement to notify affected individuals, namely where:

- organisations have taken timely remedial actions in accordance with any prescribed requirements, which renders it unlikely that the breach will result in significant harm to affected individuals; and
- the personal data that was compromised by the data breach is subject to technological protection (eg, encryption) such that the data breach is unlikely to result in significant harm to the affected individuals.

Organisations must also not notify affected individuals if instructed by a prescribed law enforcement agency or directed not to do so by the PDPC, for example, in circumstances where notification may compromise investigations or prejudice enforcement efforts.

The Personal Data Protection (Notification of Data Breaches) Regulations 2021 set out further prescribed requirements relating to data breach notifications, including the contents of the notification to the PDPC and the categories of prescribed personal data that are deemed to result in significant harm to the affected individual.

For more information, organisations may refer to the PDPC's Guide on Managing and Notifying Data Breaches under the PDPA (revised 15 March 2021).

Updates and trends

Joint Guide to ASEAN MCCs and EU SCCs

On 24 May 2023, the PDPC released the Joint Guide to ASEAN Model Contractual Clauses and EU Standard Contractual Clauses (the Joint Guide), which was a collaborative effort between the Association of Southeast Asian Nations and the EU launched at the Computers, Privacy and Data Protection Conference in Brussels.

The Joint Guide provides a helpful comparison between model contractual clauses (MCCs) and standard contractual clauses (SCCs) for organisations looking to transfer or receive consumer data from overseas partners. Organisations already familiar with the MCCs can use the Joint Guide as a reference in their contractual negotiations on data transfers with their EU business partners.

38 There is no specified time period within which to notify affected individuals in the PDPA and the Personal Data Protection Commission's guidelines; however, generally, the time frame must be a reasonable one, taking into account Section 11(1) of the PDPA which states that 'In meeting its responsibilities under [the PDPA], an organisation must consider what a reasonable person would consider appropriate in the circumstances.'

Surveillance laws

The PDPA does not have any express provisions on surveillance. Organisations may generally collect, use and disclose personal data without an individual's consent, if required or authorised to do so under any written law or if any exception in the PDPA applies.

Singapore also does not have a single dedicated law providing for public authorities' right of surveillance or access to information (including personal data). Each piece of Singapore legislation (eg, the Official Secrets Act 1935, the Criminal Procedure Code 2010 and Prevention of Corruption Act 1960) sets out its own range of powers of investigation to be exercised by the competent authority, with corresponding thresholds and restrictions in view of the objective pursued. These statutory laws do not target personal data processing per se.

Case studies

As at 30 June 2023, the PDPC has released 236 enforcement decisions, which are helpful in illustrating how the PDPA is to be interpreted. Some case studies are discussed below.

Breach of protection obligation by SingHealth and IHiS

In a decision on 15 January 2019, the PDPC imposed its highest financial penalties to date of S$250,000 and S$750,000 respectively on Singapore Health Services Pte Ltd (SingHealth) and Integrated Health Information Systems Pte Ltd (IHiS), for breaching their data protection obligations under the PDPA.[39] This unprecedented data breach, which arose from a cyberattack on SingHealth's patient database system, caused the sensitive personal data of almost 1.5 million patients to be compromised.

Court of Appeal clarifies right to private action under PDPA

In September 2022, the Court of Appeal handed down the significant decision in *Reed, Michael v Bellingham, Alex (Attorney-General, intervener)*.[40] Importantly, the Court of Appeal held that emotional distress is sufficient to constitute the 'loss or damage' required to find a private action under section 480(1) of the PDPA, reversing the Singapore High Court's earlier decision on the matter.

39 *Re Singapore Health Services Pte Ltd and another* [2019] SGPDPC 3.
40 *Reed, Michael v Bellingham, Alex (Attorney-General, intervener)* [2022] SGCA 60.

The Court of Appeal also held that, in contrast, the loss of control of personal data does not on its own constitute such loss or damage.

Capgemini held liable and damages awarded to Razer over data leak

On 9 December 2022, gaming hardware company, Razer, won its lawsuit against an IT vendor, Capgemini, over cybersecurity breaches and a related data leak involving 147,000 customer accounts. Razer was awarded US$6.5 million in damages by the Singapore High Court.[41] The dispute arose as a result of the misconfiguration of a server file, which resulted in a leak of Razer's non-public customer data involving shipping information and order details of customers worldwide.

AI Framework

On 21 January 2020, the PDPC published the second edition of its Model AI Governance Framework (the AI Framework). This is an accountability-based framework that helps to chart the language and frame discussions around harnessing artificial intelligence (AI) in a responsible way. Key changes in the second edition include the addition of industry examples in each section of the AI Framework to clearly illustrate how organisations have implemented AI governance practices.

The AI Framework is accompanied by the 'Compendium of Use Cases' and the 'Implementation and Self-Assessment Guide for Organizations'.

Launch of AI governance testing framework and toolkit

On 25 May 2022, the IMDA and the PDPC launched AI Verify, the world's first AI governance testing framework and toolkit, for companies that wish to demonstrate their deployment of responsible AI. AI Verify is currently available as a minimum viable product for system developers and owners who want to be more transparent about the performance of their AI systems through a combination of technical tests and process checks.

On 7 June 2023, IMDA set up the AI Verify Foundation to harness the collective power and contributions of the global open source community to develop AI Verify. The Foundation seeks to boost AI testing capabilities and assurance to meet the needs of companies and regulators globally. The Foundation has more than 60 general members, with seven premier members – Aicadium, Google,

41 *Razer (Asia-Pacific) Pte Ltd v Capgemini Singapore Pte Ltd* [2022] SGHC 310.

IBM, IMDA, Microsoft, Red Hat and Salesforce – that will set strategic directions and a development roadmap for AI Verify.

Lim Chong Kin
Drew & Napier LLC

Lim Chong Kin is the managing director of Drew & Napier's corporate and finance department. He heads the telecommunications, media and technology (TMT) and competition, consumer and regulatory practices, and is co-head of the data protection, privacy and cybersecurity practice.

Chong Kin is cited by many publications as a leading lawyer in the fields of TMT, and regulatory, antitrust and competition. He is highly regarded by his peers, clients and rivals for his expertise and is lauded for being a 'very technically proficient and commercially savvy lawyer', who has 'unique insights into policy direction and interpretation' and 'understands regulatory thinking like no other lawyer in the field'.

Chong Kin acts for various clients, including household-name technology companies, payment systems providers, cloud service providers, media conglomerates, telecommunication providers and e-commerce start-ups. His broad experience includes supporting regulators to develop first-of-their-kind regulatory frameworks. He has acted as external counsel to the then Infocomm Development Authority in liberalising the telecoms industry and developing the Telecom Competition Code, and the then Media Development Authority in developing the Media Market Conduct Code. He has also supported the Personal Data Protection Commission in numerous projects to administer the Personal Data Protection Act 2012. Chong Kin continues to advise clients in cutting-edge ICT, data protection and cybersecurity matters.

Anastasia Su-Anne Chen
Drew & Napier LLC

Anastasia Su-Anne Chen is a director in Drew & Napier's corporate and finance department. Her key areas of practice are data protection, privacy, cybersecurity, and technology, media, and telecommunications (TMT).

Before joining the firm, Anastasia was deputy chief counsel to Singapore's Personal Data Protection Commission (PDPC) and Infocomm Media Development Authority (IMDA) for over nine years. She was lead counsel for PDPC's matters, IMDA's procurement and IP portfolios, as well as the legal adviser to IMDA's Data Administration Group. This included advising on the administration, application and enforcement of Singapore's Personal Data Protection Act 2012 (PDPA).

Significant national projects that she has worked on include the amendments to the PDPA, which came into effect on 1 February 2021, and Singapore's participation and implementation of the APEC Cross Border Privacy Rules System.

Anastasia has broad experience in data protection compliance programmes and documentation, cross-border data transfers, the coordination of multi-jurisdictional projects and data breach management. She also advises on related TMT matters, such as regulatory issues in respect of data centres and the use of artificial intelligence.

DREW & NAPIER

Drew & Napier's work in data protection, privacy and cybersecurity precedes the advent of Singapore's Personal Data Protection Act 2012 and Cybersecurity Act 2018. Our expertise extends beyond general data protection law to sectoral frameworks, in particular, in the telecommunications, media and technology; financial; and healthcare sectors. Over the past decade, Drew & Napier has been one of the leading practices in this field, having worked on a number of important matters for our clients.

We have been at the forefront of data protection laws in Singapore, given that we were involved with the Infocomm Media Development Authority and Personal Data Protection Commission (IMDA/PDPC) in setting up the implementing data protection laws in Singapore. We continue to represent the IMDA/PDPC in advisory, enforcement and policy work.

We also regularly act for a wide range of clients on a variety of data protection matters, including the implementation of group-wide data protection compliance programmes, the localisation of global data privacy policies, data protection training programmes, advising companies on dealing with data breaches, conducting regulatory risk audits, and addressing ad hoc queries.

10 Collyer Quay
10th Floor Ocean Financial Centre
Singapore 049315
Tel: +65 6531 4110
Fax: +65 6535 4864

www.drewnapier.com

Lim Chong Kin
chongkin.lim@drewnapier.com

Anastasia Su-Anne Chen
anastasia.chen@drewnapier.com