GDR INSIGHT

HANDBOOK 2021

HANDBOOK
2021

Reproduced with permission from Law Business Research Ltd
This article was first published in December 2020
For further information please contact Natalie.Clarke@lbresearch.com

Published in the United Kingdom
by Global Data Review
Law Business Research Ltd
Meridian House, 34–35 Farringdon Street, London, EC4A 4HL, UK

www.globaldatareview.com

To subscribe please contact subscriptions@globaldatareview.com

ISBN: 978-1-83862-266-4

Printed and distributed by Encompass Print Solutions
Tel: 0844 2480 112

Contents

Privacy

Cybersecurity

Data in practice

PREFACE

Global Data Review is delighted to publish this second edition of the *GDR Insight Handbook*.

The handbook 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 legislation that a ects how businesses handle their data.

The book's comprehensive format provides in-depth analysis of the global developments in key areas of data law and their implications for multinational businesses. Experts from across Europe, the Americas and Asia consider the latest trends in privacy and cybersecurity. Attention is also given to new legislation in the United States that regulates the use of arti cial intelligence, and strict data localisation rules emerging in jurisdictions such as China. The handbook provides practical guidance on the implications for companies wishing to buy or sell datasets, and the intersection of privacy, data and antitrust. A chapter is dedicated to the use of arti cial intelligence in cross-border forensic investigations.

In preparing this report, Global Data Review has worked with leading data lawyers and consultancy experts from around the world and we are grateful for all their cooperation and insight.

The information listed is correct as at November 2020. Although every e ort has been made to ensure that all the matters of concern to readers are covered, data law is a complex and fast-changing eld of practice, and therefore speci c legal advice should always be sought. Subscribers to Global Data Review will receive regular updates on any changes to relevant laws over the coming year.

We would like to thank all those who have worked on the research and production of this publication.

Global Data Review
London
November 2020

PART 1

Privacy

SINGAPORE: PRIVACY

Lim Chong Kin and Janice Lee
Drew & Napier LLC

Key statutes, regulations and adopted international standards

The Personal Data Protection Act 2012 (No. 26 of 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 III to VI (the Data Protection Provisions) set out the general obligations of organisations with regard to their management of personal data, while Part IX 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 2014;
- the Personal Data Protection (Composition of Offences) Regulations 2013;
- the Personal Data Protection (DNC Registry) Regulations 2013;
- the Personal Data Protection (Enforcement) Regulations 2014; and
- the Personal Data Protection (Appeal) Regulations 2015.

The Singapore data protection authority, the Personal Data Protection Commission (PDPC), has also issued a number of advisory guidelines detailing how it will interpret the provisions of the PDPA. This guidance ranges from general advisory 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 to industry-led guidelines for the insurance industry.

The PDPA is currently undergoing its first comprehensive review since its enactment in 2012. On 14 May 2020, the Ministry of Communications and Information (MCI) and the PDPC launched a public consultation on the proposed Personal Data Protection (Amendment) Bill 2020 (PDP (Amendment) Bill), which follows in the wake of three public consultations held between 2017 and 2019. As at the time of writing, the PDP (Amendment) Bill yet to be introduced in Parliament and the proposed amendments have yet to take effect.

Aside from the PDPA, a number of other 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 (Chapter 19). The Monetary Authority of Singapore (MAS) also 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.

Other examples include the healthcare sector, where the confidentiality of medical information and the retention of medical records are governed by the Private Hospitals and Medical Clinics Act (Chapter 248). In the telecommunications sector, the Telecoms Competition Code issued under the Telecommunications Act (Chapter 323) regulates the telecommunications licensees' use of end-user service information.

Other legislation that may have an indirect impact on data protection include the Computer Misuse Act (Chapter 50A), which contains offences for the unauthorised access or modification of computer material and the unauthorised use or interception of computer services. The Cybersecurity Act (No. 9 of 2018) 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.

However, 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 other written laws will prevail.

Adopted international standards

Singapore participates in the Asia-Pacific Economic Cooperation (APEC)'s Cross-Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP) systems. 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 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 Info-communications Media Development Authority (IMDA). Sectoral regulators separately enforce the data protection obligations within their relevant sectors.

With respect to enforcement of the PDPA, the PDPC may direct organisations to:[1]

- stop collecting, using or disclosing personal data in contravention of the PDPA;
- destroy personal data collected in contravention of the PDPA;
- provide access to or correct personal data, or reduce or make a refund of any fee charged for any access or correction request; or
- pay a financial penalty not exceeding S$1 million (under the proposed PDP (Amendment) Bill, the present financial penalty cap is raised to up to 10 per cent of an organisation's annual gross turnover in Singapore or S$1 million, whichever is higher).

In carrying out its investigative functions, the PDPC is empowered to:[2]

- require any organisation to produce any specified document or to provide any specified 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.

The PDP (Amendment) Bill aims to 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 be imposed on individuals and organisations that obstruct or hinder the investigations of 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 for the offence of providing any false or misleading statements or information to the PDPC.

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; or issue an expedited breach decision in certain circumstances where there is an upfront, voluntary admission of liability for breaching relevant obligations under the PDPA.

The PDPC has been active in its enforcement of the PDPA. As at 14 August 2020, the PDPC had issued a total of 146 decisions, with a significant majority relating to breaches of the protection obligation. Out of all these 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.

1 Section 29(2) of the PDPA.

2 Section 50(2) read with the Ninth Schedule to the PDPA.

3 Section 51 of the PDPA.

The effect of local laws on foreign businesses

The PDPA applies to all organisations regardless of whether they were formed or are recognised under Singapore law, or are resident or with an office or place of business in Singapore. As such, the applicability of the PDPA can extend to foreign businesses. For example, in *Re Cigna Europe Insurance Company SA-NV* [2019] SGPDPC 18, 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. Ultimately, however, the PDPC found that the organisation was not in breach of its data protection obligations.

The PDPC is also a participant of the APEC Cross-border Privacy Enforcement Arrangement, which is a framework for the voluntary sharing of information and provision of assistance for privacy enforcement-related activities among privacy enforcement authorities.

Core principles on personal data

Definition of personal data

'Personal data' is broadly defined under the PDPA as 'data, whether true or not, about an individual who can be identified from that data, or from that data and other information to which the organisation has or is likely to have access'.

In addition, the PDPC refers to certain types of personal data that, on its own, can identify an individual, as 'unique identifiers'. Examples would include full names; National Registration Identity Card (NRIC) and passport numbers; personal mobile phone numbers; facial image of an individual; voice of an individual; fingerprint; DNA profile; and iris image.

While the PDPA does not distinguish between specific categories of 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 NRIC numbers, insurance data, medical data, financial data and children's data.[4]

Data protection obligations

The Data Protection Provisions contain nine main obligations that organisations are required to comply with if they undertake activities relating to the collection, use or disclosure of personal data.

Consent obligation

An organisation must obtain the consent of an individual before collecting, using or disclosing his personal data for a purpose, unless an exception in the Second, Third or Fourth Schedule to the PDPA applies.[5] Some examples of exceptions to consent would be where the personal

4 See *Re Aviva Ltd* [2017] SGPDPC 14; *Re Credit Counselling Singapore* [2017] SGPDPC 18; *Re Singapore Taekwondo Federation* [2018] SGPDPC 17; and *Re AIA Singapore Private Limited* [2019] SGPDPC 20.

5 Section 13 of the PDPA.

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 PDP (Amendment) Bill seeks to introduce two new exceptions to the consent requirement, the 'legitimate interests'[6] and 'business improvement'[7] exceptions.

For consent to be considered validly given, the organisation must first inform the individual of the purposes for which his or her personal data will be collected, used or disclosed, and these purposes have to be what a reasonable person would consider appropriate in the circumstances. Fresh consent would need to be obtained where personal data collected is to be used for a different purpose to which the individual originally consented.

Consent may also be deemed to have been given where an individual has voluntarily provided his or her data to an organisation for a purpose, and it is reasonable that the individual do so.[8] The onus is on the organisation to establish that the individual was aware of the purposes for which the personal data was provided. The PDP (Amendment) Bill also seeks to expand the concept of deemed consent under the PDPA to include deemed consent by contractual necessity[9] and deemed consent by notification.[10]

Consent obtained via 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 such consent is beyond what is reasonable to provide the product or service to the individual; and where false or misleading information is provided, or deceptive or misleading practices are used, in order to obtain or attempt to obtain the individual's consent for collecting, using or disclosing personal data.[11]

Individuals may also withdraw any consent given or deemed to have been given at any time upon giving reasonable notice to the organisation.[12]

6 The 'legitimate interests' exception enables organisations to collect, use or disclose personal data without consent in circumstances where there is a need to protect legitimate interests that will have economic, social, security or other benefits for the public (or a section thereof). Such benefits to the public must outweigh any adverse impact to the individual, and organisations wishing to rely on this 'legitimate interests' basis must conduct fulfil certain requirements (eg, conducting a risk and impact assessment).

7 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.

8 Section 15 of the PDPA.

9 For deemed consent by contractual necessity, consent is deemed to have been given for the use and 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.

10 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.

11 Section 14(2) of the PDPA.

12 Section 16 of the PDPA.

Notification obligation

Organisations are obliged to inform individuals of the purposes for the collection, use or disclosure of his or her 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.[13]

Access and correction obligations

Under the access obligation, an organisation must allow an individual to access his or her 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 .[14] 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 also 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.[15] 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.

The PDP Regulations 2014 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.[16]

13 Section 18 of the PDPA.
14 Section 21 of the PDPA.
15 Section 22 of the PDPA.
16 Section 23 of the PDPA.

Protection obligation

An organisation must make reasonable security arrangements to protect personal data in its possession or under its control, in order to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.[17]

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.[18]

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 the PDP Regulations 2014 to ensure that the transferred personal data will be accorded a standard of protection that is comparable to that under the PDPA.[19]

Organisations must ensure that the recipients of that personal data are bound by legally enforceable obligations to provide to the transferred personal data a standard of protection that is at least comparable to the protection under the PDPA. These 'legally enforceable obligations' include obligations imposed under law, contract or binding corporate rules, or any other legally binding instrument.[20]

Accountability obligation

Organisations must undertake and demonstrate responsibility for the personal data in its possession or control.[21] This includes developing and implementing data protection policies; communicating to and informing their staff of these policies; implementing processes and practices that are necessary to meet their obligations under the PDPA; making information about its 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.[22]

The PDPC also recommends that organisations conduct a data protection impact assessment (DPIA) to assess if 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.

17 Section 24 of the PDPA.
18 Section 25 of the PDPA.
19 Section 26 of the PDPA.
20 Regulation 9(1) of the PDP Regulations 2014.
21 Section 11 of the PDPA. Previously known as the openness obligation.
22 Section 12 of the PDPA.

Data intermediaries

The PDPA also 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.[23] When an organisation employs a data intermediary to process personal data on its behalf and for its purposes, organisations have the same obligation under the PDPA as if the personal data were processed by the organisation itself.

Automated processing, profiling and data analytics

While the PDPC does not have express provisions on automated individual decision-making, data analytics and profiling, insofar as an organisation wishes to carry out automated processes, it will need to ensure that it complies with the Data Protection Provisions and obtain the necessary consent from the individuals in question unless an exception under the PDPA applies.

Communications and marketing

Sending specified messages

The DNC Provisions[24] 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 (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;
- land or an interest in land; or
- a business or investment opportunity; to advertise or promote a supplier or provider, or prospective supplier or provider for the above or any other prescribed purpose.

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

23 Section 4(2) of the PDPA.

24 The PDP (Amendment) Bill intends to make certain changes to the DNC Provisions, which includes: inserting a new Part IXA 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 DNC register query results to organisations on whose behalf they are checking the register.

Under section 43 of the PDPA, an organisation that intends to send a specified message to a user or subscriber of a Singapore 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 writing or other forms accessible for future reference.

When sending marketing communications to a Singapore telephone number, organisations must comply with the 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 conceal or withhold from the recipient the identity of the caller.[25]

Certain senders that are in an ongoing relationship with individuals may be exempted from the obligation to check the DNC Registry before sending specified text or fax messages related to the subject of the ongoing relationship under the Personal Data Protection (Exemption from section 43) Order 2013 (Exemption Order). Conversely, one-off transactions are insufficient to establish an ongoing relationship, and organisations may not rely on the Exemption Order once the ongoing relationship has ceased.

Spam Control Act

Aside from the DNC Provisions, the Spam Control Act (Chapter 311A) (SCA) governs the control of spam, namely unsolicited commercial communications sent in bulk by electronic mail or by text or multimedia messaging to mobile telephone numbers.[26] 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, which include providing:

- the contact information of the sender through which the recipient can submit an unsubscribe request;
- a clear statement in English informing the recipient of his or her right to make an unsubscribe request;
- if the message has a subject field, a correct and accurate title in the subject field that reflects the message's content;
- the tag <ADV> before the title of the message or, where there is no title, before the first word of the actual message;
- header information that is true and not misleading; and

25 Sections 44 and 45 of the PDPA.

26 The PDP (Amendment) Bill intends to make certain changes to the SCA, which includes amending it to cover messages sent to Instant Messaging (IM) accounts via IM platforms, including platforms such as Telegram and WeChat.

- an accurate and functional email address or telephone number by which the sender can be readily contacted.

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 under the access and correction obligations. In addition, the draft PDP (Amendment) Bill proposes to introduce a new Data Portability Obligation, which requires an organisation to, at the request of an individual, transmit personal data that is in the organisation's possession or under its control, to another organisation in a commonly used machine-readable format. Nonetheless, it is contemplated that the obligation will be subject to various exceptions and the fulfilment of certain conditions.

Individuals also have the right to give and withdraw consent at any time by giving reasonable notice, unless it would frustrate the performance of a legal obligation.[27] 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, but may only commence an action after the PDPC's decision has become final and the organisation has no further right of appeal. [28]

The role of the data protection officer

As part of the accountability obligation, it is mandatory for organisations to appoint a DPO.[29] The responsibility of the DPO is to ensure that the organisation complies with the PDPA by developing and implementing policies and processes 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 and cannot be delegated to the DPO.

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 under the notification obligation. This person may also be the DPO.[30] 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

27 Section 16 of the PDPA.
28 Section 32(1) of the PDPA.
29 Section 11(3) of the PDPA.
30 Section 11(5) of the PDPA.

that the business contact information of this person should be readily accessible from Singapore, operational during Singapore business hours and if telephone numbers are used, be Singapore telephone numbers.

Data protection breaches

There is currently no mandatory data breach notification requirement or procedure under the PDPA, although the PDPC has issued certain guidelines encouraging notification to the PDPC and affected individuals in certain circumstances.

However, the draft PDP (Amendment) Bill seeks to introduce a mandatory data breach notification obligation. In the draft Bill, organisations are required to notify the PDPC of a data breach (as defined in the draft Bill) that is likely to result in significant harm or impact to the individuals to whom the data relates (eg, if it affects any prescribed class of personal data); or is of a significant scale (ie, if 500 or more individuals are affected).

The draft Bill also provides that where an organisation has reason to believe that a data breach has occurred, it must conduct, in a reasonable and expeditious manner and in accordance with any prescribed requirements, an assessment as to whether it is notifiable. Upon determining that it meets the notification threshold, organisations must notify the PDPC as soon as practicable, but in any case, no later than three calendar days after making such a determination.

Subject to certain prescribed exceptions, organisations are required to, on or after notifying the PDPC, notify affected individuals if the data breach is likely to result in significant harm or impact to the individuals.

Updates and trends

Model AI governance framework

On 21 January 2020, the PDPC published the second edition of its Model Artificial Intelligence (AI) Governance Framework (AI Framework). This is an accountability-based framework that helps to chart the language and frame the discussions around harnessing AI in a responsible way. The key changes in the second edition includes 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 a Compendium of Use Cases and an Implementation and Self-Assessment Guide for Organisations.

Proposed changes to legislation

As stated above, the PDPA is currently undergoing its first comprehensive review of the PDPA since its enactment in 2012. On 14 May 2020, the MCI and the PDPC issued the proposed Personal Data Protection (Amendment) Bill and the accompanying public consultation paper, and sought comments on the draft Bill from 14 to 28 May 2020. The proposed amendments aim to strengthen public trust, enhance business competitiveness, and provide greater organisational accountability and assurance to consumers.

Surveillance laws

While 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 the PDPA or other written law or if any exception in the PDPA applies.

Singapore also has other piecemeal legislation relating to state interception of communications and the monitoring and surveillance of individuals for national security purposes.

In terms of surveillance via closed-circuit television (CCTV) cameras, unless an exception under the PDPA applies, organisations are required to inform individuals of the purposes for which their personal data will be collected, used or disclosed in order to obtain their consent. As such, organisations that install CCTV cameras in their premises are required to put up notices indicating that CCTV cameras are operating in the premises, state the purpose of such surveillance if such purpose may not be obvious to the individual, and also if both audio and video recordings are taking place in order to obtain consent for the collection, use, or disclosure of personal data from the CCTV footage. In addition, organisations that operate unmanned aircraft and aerial vehicles (ie, drones) equipped with photography, video or audio recording capabilities will need to comply with the PDPA insofar as the drones are likely to capture the personal data of individuals.[31]

Case studies

Since 2016, the PDPC has released 146 enforcement decisions that are helpful in illustrating how the PDPA is to be interpreted. We have selected several case studies below.

Breach of accountability, protection, and transfer limitation obligations by Bud Cosmetics Pte Ltd[32]

On 3 January 2019, the PDPC issued a financial penalty of S$11,000 to a skincare retailer, Bud Cosmetics, which was found to have breached the accountability, protection, and transfer limitation obligations. In this case, the PDPC shed some light as to the application of the transfer limitation obligation as set out in section 26 of the PDPA. Broadly, with respect to the transfer of personal data outside of Singapore, organisations should undertake an assessment of the personal data protection laws in those jurisdictions to determine if the protections afforded to personal data are comparable with the protections under the PDPA. If this is not the case, the organisation should then consider whether it can impose contractual safeguards to ensure such comparable protection.

31 See Advisory Guidelines on the PDPA for Selected Topics at Chapter 4.

32 *Re Bud Cosmetics* [2019] SGPDPC 1..

Breach of accountability obligation by Xbot Pte Ltd[33]

On 20 June 2019, the PDPC issued a warning to Xbot Pte Ltd, an organisation which developed and operated a mobile app and associated website providing access to a database of residential property transactions. The organisation was found to have breached the accountability obligation. This case illuminates what is meant by the "policies and practices" required under section 12 of the PDPA. According to the PDPC, they refer to both external published data protection policy informing individuals and the internal policies and practices meant for the organisation's employees; and the specific internal policies and practices required for a particular organisation would depend on various factors, including for instance, the types and amount of personal data collected by the organisation.

Breach of protection obligation by SingHealth Services Pte Ltd and Integrated Health Information Systems Pte Ltd[34]

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, for breaching their data protection obligations under the PDPA in a decision on 15 January 2019. This unprecedented data breach, which arose from a cyber attack on SingHealth's patient database system, caused the sensitive personal data of almost 1.5 million patients to be compromised.

Breach of protection obligation by The Central Depository (Pte) Limited[35]

On 3 August 2019, the PDPC published a decision pertaining to the Central Depository's breach of the protection obligations, which culminated in a financial penalty of S$30,000. The PDPC found that prior to migrating personal data from an older IT system to a newer IT system, the organisation had failed to conduct proper and adequate pre-launch testing of the newer IT system. This failure led to the dividend cheques of some CDP account holders being mailed to outdated addresses, resulting in the unauthorised disclosure of these CDP account holders' personal data.

33 *Re Xbot Pte Ltd* [2019] SGPDPC 19.

34 *Re Singapore Health Services Pte Ltd and another* [2019] SGPDPC 3.

35 *Re The Central Depository (Pte) Limited* [2020] SGPDPC 12.

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 he 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 telecommunications, media and technology; 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 a wide range of 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 Infocomm Development Authority in liberalising the telecom industry and developing the Telecom Competition Code, and the 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. To date, Chong Kin continues to advise clients in cutting-edge ICT, data protection, and cybersecurity matters.

Janice Lee
Drew & Napier LLC

Janice's key practice areas are corporate and commercial law, with an emphasis on data protection, TMT and regulatory matters.

Janice assists clients on Singapore data protection law compliance, including reviewing contractual agreements and policies, conducting training and audits, and advising on enforcement issues relating to security, access, monitoring and data breaches. In addition, Janice regularly advises private entities and statutory boards on a range of contractual, corporate advisory and regulatory matters.

Janice is a Certified Information Privacy Professional for Europe (CIPP/E) and a Certified Information Privacy Manager (CIPM).

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 last 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 Info-communications Media Development Authority (IMDA)/Personal Data Protection Commission (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

Janice Lee
janice.lee@drewnapier.com

The GDR Insight Handbook 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.

The book's comprehensive format provides in-depth analysis of the developments in key areas of data law. Experts from across Europe, the Americas and Asia consider the latest trends in privacy and cybersecurity, providing practical guidance on the implications for companies wishing to buy or sell data sets, and the intersection of privacy, data and antitrust.

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

an LBR business

ISBN 978-1-83862-266-4