THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

SEVENTH EDITION

Editor
Alan Charles Raul

THE LAWREVIEWS

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

SEVENTH EDITION

Reproduced with permission from Law Business Research Ltd
This article was first published in September 2020
For further information please contact Nick.Barette@thelawreviews.co.uk

Editor
Alan Charles Raul

THE LAWREVIEWS

PUBLISHER
Tom Barnes

SENIOR BUSINESS DEVELOPMENT MANAGER
Nick Barette

BUSINESS DEVELOPMENT MANAGER
Joel Woods

SENIOR ACCOUNT MANAGERS
Pere Aspinall, Jack Bagnall

ACCOUNT MANAGERS
Olivia Budd, Katie Hodgetts, Reece Whelan

PRODUCT MARKETING EXECUTIVE
Rebecca Mogridge

RESEARCH LEAD
Kieran Hansen

EDITORIAL COORDINATOR
Gavin Jordan

PRODUCTION AND OPERATIONS DIRECTOR
Adam Myers

PRODUCTION EDITOR
Claire Ancell

SUBEDITOR
Martin Roach

CHIEF EXECUTIVE OFFICER
Nick Brailey

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

www.TheLawReviews.co.uk

ISBN 978-1-83862-485-9

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

© 2020 Law Business Research Ltd

ACKNOWLEDGEMENTS

The publisher acknowledges and thanks the following for their assistance throughout the preparation of this book:

ADVOKAADIBÜROO NORDX LEGAL

ALLENS

ANJIE LAW FIRM

ASTREA

AZEVEDO SETTE ADVOGADOS

BOGSCH & PARTNERS LAW FIRM

BOMCHIL

BTS&PARTNERS

CLEMENS

CTSU – SOCIEDADE DE ADVOGADOS

GREENBERG TRAURIG LLP

K&K ADVOCATES

nNOVATION LLP

NOERR

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SK CHAMBERS

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

VUKINA & PARTNERS LTD

WALDER WYSS LTD

WINHELLER ATTORNEYS AT LAW & TAX ADVISORS

CONTENTS

Chapter 24

SINGAPORE

Yuet Ming Tham[1]

I OVERVIEW

In 2019 and 2020, Singapore continued to develop its data protection, cybercrime, and cybersecurity regimes. As set out in Singapore's Cyber Landscape 2019 report,[2] the government focused on four pillars of strategy to protect the country from cyberthreats and reinforce Singapore's standing as a leading information systems hub. It aimed to: (1) build a resilient infrastructure; (2) create a safer cyberspace environment; (3) develop a vibrant cybersecurity ecosystem; and (4) strengthen international partnerships. The key legal components in this strategy include the Personal Data Protection Act 2012 (PDPA), Singapore's first comprehensive framework established to ensure the protection of personal data, the Computer Misuse Act (CMA) to combat cybercrime and other cyberthreats, and the Cybersecurity Act 2018 (the Cybersecurity Act), which focuses on protecting Singapore's Critical Information Infrastructure (CII) in 11 critical sectors and establishing a comprehensive national cybersecurity framework.

In this chapter, we will outline the key aspects of the PDPA, CMA and the Cybersecurity Act. The chapter will place particular emphasis on the PDPA, including a brief discussion of the key concepts, the obligations imposed on data handlers, and the interplay between technology and the PDPA. Specific regulatory areas such as the protection of minors, financial institutions, employees and electronic marketing will also be considered. International data transfer is particularly pertinent in the increasingly connected world; how Singapore navigates between practical considerations and protection of the data will be briefly examined. We also consider the enforcement of the PDPA in the event of non-compliance.

II THE YEAR IN REVIEW

i PDPA developments

There were a number of significant developments related to the PDPA and the Personal Data Protection Commission (PDPC – the body set up to administer and enforce the PDPA) from July 2019 to June 2020.

The PDPC increasingly emphasises the principle of 'accountability' in the context of personal data protection and has provided guidance on how organisations may demonstrate accountability for personal data in their care. On 15 July 2019, the PDPC published the

1 Yuet Ming Tham is a partner at Sidley Austin LLP.

2 See Singapore's Cyber Landscape 2019, Cybersecurity Agency of Singapore, issued on 26 June 2020, available at https://www.csa.gov.sg/-/media/csa/documents/publications/singaporecyberlandscape2019.pdf.

Guide to Accountability under the PDPA and updated the PDPC's Advisory Guidelines to include a section on 'Accountability Obligation' in place of the 'Openness Obligation' under Section 11 of the PDPA (which relates to, among other things, obligations on organisations to make available information about their data protection policies and practices). Other recent guidance includes the second edition of the Model AI Governance Framework, released by the PDPC on 21 January 2020, which outlines an accountability-based framework and guidelines by which organisations can deploy AI solutions responsibly. On 17 July 2019, a new Data Protection Officer (DPO) Competency Framework and Training Roadmap was published to clarify the core competencies and proficiency levels for a DPO.

On 17 July 2019, the PDPC announced that the Infocomm Media Development Authority (IMDA) has been appointed as Singapore's Accountability Agent for the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP) Systems certifications. With this appointment, organisations can now be certified under the APEC CBPR and PRP Systems for accountable data transfers across borders to other certified organisations. Following this, the PDPC amended the Personal Data Protection Regulations on 2 June 2020 to formally recognise the APEC CBPR System and PRP System certifications as one of the accepted modes for overseas data transfers. The PDPC also entered into a Memorandum of Understanding (MOU) with the Philippines' National Privacy Commission and the Office of the Australian Information Commissioner (OAIC) on 9 September 2019 and 25 March 2020 respectively. The MOUs set out, among other things, a framework for cooperation for the mutual exchange of information and assistance in joint investigations, and the development of compatible mechanisms to facilitate cross-border data flows such as participation in the APEC CBPR System.

In September and October 2019, the PDPC published revisions to a number of guidelines. This includes revisions to the PDPC's Guide to Notification, which outlines best practices for notifying individuals about an organisation's personal data protection policies and practices. The revised guide includes a section on key considerations in developing notifications and new examples, including dynamic consent and just-in-time notifications. The PDPC also revised Chapter 6 on 'Organisations' and Chapter 15 on 'Access and Correction Obligations' of the Advisory Guidelines on Key Concepts in the PDPA, and introduced a new chapter on 'Cloud Services' in the Advisory Guidelines on the PDPA for Selected Topics.

As further discussed in Part X, from 14–28 May 2020, the Ministry of Communications and Information and the PDPC launched an online public consultation on the proposed amendments to the PDPA and related amendments to the Spam Control Act.

ii CMA developments and the Cybersecurity Act

Cybercrime and cybersecurity are regulated under the CMA (formerly known as the Computer Misuse and Cybersecurity Act) and the Cybersecurity Act, both of which are closely linked.

The CMA was amended in 2013 and again in 2017 to strengthen the country's response to national-level cyberthreats. The amendments broadened the scope of the CMA by criminalising certain conduct not already covered by the existing law and enhancing penalties in certain situations (for example, the amended CMA criminalises the use of stolen data to carry out a crime even if the offender did not steal the data himself or herself, and prohibits the use of programs or devices used to facilitate computer crimes, such as malware or code

crackers). The amendments also extended the extraterritorial reach of the CMA by covering actions by persons targeting systems that result in, or create a significant risk of, serious harm in Singapore, even if the persons and systems are both located outside Singapore.

In keeping with the government's emphasis on safeguarding critical information infrastructure, the Cybersecurity Act was enacted on 31 August 2018. The Cybersecurity Act creates a framework for the protection of CII against cyberthreats, creates the Commissioner of Cybersecurity with broad powers to administer the Cybersecurity Act, establishes a licensing scheme for providers of certain cybersecurity services, and authorises measures for the prevention, management, and response to cybersecurity incidents in Singapore.

While there have been no significant legislative developments in this area since 2018, cross-border enforcement of the Cybersecurity Act remains a challenging problem, particularly for cloud-based service providers. Singapore has signed MOUs and entered into cooperation arrangements with multiple foreign governments to facilitate international collaboration to address cybersecurity. These MOUs and cooperation arrangements were with Australia, Canada, India, France, Germany, Japan, the Republic of Korea, the Netherlands, New Zealand, the United States and the United Kingdom.

iii Recent developments and regulatory compliance

Although the developments with the CMA and the Cybersecurity Act represent significant milestones in Singapore's overall cybersecurity strategy, the key compliance framework from the perspective of companies and organisations remains at this point with data protection and privacy. The CMA is primarily a criminal statute, and the government has not issued any regulations or guidelines for the CMA. The Cybersecurity Act imposes a number of legal requirements on CII owners and cybersecurity service providers, but until the government issues implementing regulations or advisory guidance regarding these new requirements, organisations' focus will be on the PDPA and its related regulations, subsidiary legislation and advisory guidelines.[3]

Singapore experienced its most serious data privacy breach yet in July 2018 when hackers infiltrated Singapore Health Services' (SingHealth) databases, compromising the personal data of 1.5 million patients, including the outpatient prescriptions of Prime Minister Lee Hsien Loong. The PDPC fined Integrated Health Information Systems (the IT agency responsible for Singapore's public healthcare sector) S$750,000 and SingHealth S$250,000 for breaching their data protection obligations leading to the breach. Since then, there have been a number of high-profile data breach incidents, as highlighted in Part VII.

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

The PDPA framework is built around the concepts of consent, purpose and reasonableness. The main concept may be summarised as follows: organisations may collect, use or disclose personal data only with the individual's knowledge and consent (subject to certain exceptions) for a purpose that would be considered appropriate to a reasonable person in the circumstances.

3 Government agencies are not covered by the scope of the PDPA.

There is no prescribed list of 'personal data'; rather, these are defined broadly as data about an individual, whether or not they are true, who can be identified from that data or in conjunction with other information to which the organisation has or is likely to have access.[4] In addition, the PDPA does not distinguish between personal data in its different forms or mediums. Thus, there is no distinction made for personal data that are 'sensitive', or between data that are in electronic or hard copy formats. There are also no ownership rights conferred on personal data to individuals or organisations.[5] There are certain exceptions to which the PDPA would apply. Business contact information of an individual generally falls outside the ambit of the PDPA,[6] as does personal data that is publicly available.[7] In addition, personal data of an individual who has been deceased for over 10 years[8] and personal data contained within records for over 100 years is exempt.[9]

Pursuant to the PDPA, organisations are responsible for personal data in their possession or under their control.[10] 'Organisations' include individuals in Singapore, whether or not they are residents, local and foreign companies, associations and bodies (incorporated and unincorporated), whether or not they have an office or a place of business in Singapore.[11] The PDPA does not apply to public agencies.[12] Individuals acting in a personal or domestic capacity, or where they are an employee acting in the course of employment within an organisation, are similarly excluded from the obligations imposed by the PDPA.[13]

Where an organisation acts in the capacity of a data intermediary, namely an organisation that processes data on another's behalf, it would only be subject to the protection and retention obligations under the PDPA. The organisation that engaged a data intermediary's services remains fully responsible in respect of the data as if it had processed the data on its own.[14]

There is no requirement to prove harm or injury to establish an offence under the PDPA, although this would be necessary in calculating damages or any other relief to be awarded to the individual in a private civil action against the non-compliant organisation.[15]

Subsidiary legislation to the PDPA includes implementing regulations relating to the Do Not Call (DNC) Registry,[16] enforcement,[17] composition of offences,[18] requests for access to and correction of personal data and the transfer of personal data outside Singapore.[19]

4 Section 2 of the PDPA.

5 Section 5.30, Advisory Guidelines on Key Concepts in the PDPA (PDPA Key Concepts Guidelines) issued on 23 September 2013 and revised on 2 June 2020.

6 Section 4(5) of the PDPA.

7 Second Schedule Paragraph 1(c); Third Schedule Paragraph 1(c); Fourth Schedule Paragraph 1(d) of the PDPA.

8 Section 4(4)(b) of the PDPA. The protection of personal data of individuals deceased for less than 10 years is limited; only obligations relating to disclosure and protection (Section 24) continue to apply.

9 Section 4(4) of the PDPA.

10 Section 11(2) of the PDPA.

11 Section 2 of the PDPA.

12 Section 4(1)(c) of the PDPA.

13 Sections 4(1)(a) and (b) of the PDPA.

14 Section 4(3) of the PDPA.

15 Section 32 of the PDPA.

16 Personal Data Protection (Do Not Call Registry) Regulations 2013.

17 Personal Data Protection (Enforcement) Regulations 2014.

18 Personal Data Protection (Composition of Offences) Regulations 2013.

19 Personal Data Protection Regulations 2014.

There is also sector-specific legislation, such as the Banking Act, the Telecommunications Act and the Private Hospitals and Medical Clinics Act, imposing specific data protection obligations. All organisations will have to comply with PDPA requirements in addition to the existing sector-specific requirements. In the event of any inconsistencies, the provisions of other laws will prevail.[20]

The PDPC has released various advisory guidelines, as well as sector-specific advisory guidelines for the telecommunications, real estate agency, education, social services and healthcare sectors. The PDPC has also published advisory guidelines on data protection relating to specific topics such as photography, analytics and research, data activities relating to minors and employment. While the advisory guidelines are not legally binding, they provide helpful insight and guidance into problems particular to each sector or area.

ii General obligations for data handlers

The PDPA sets out nine key obligations in relation to how organisations collect, use and disclose personal data, as briefly described below.

Consent[21]

An organisation may only collect, use or disclose personal data for purposes to which an individual has consented. Where the individual provided the information voluntarily and it was reasonable in the circumstances, the consent may be presumed. Consent may be withdrawn at any time with reasonable notice.[22] The provision of a service or product must not be made conditional upon the provision of consent beyond what is reasonable to provide that product or service.

An organisation may obtain personal data with the consent of the individual from a third party source under certain circumstances. For example, with organisations that operate in a group structure, it is possible for one organisation in the group to obtain consent to the collection, use and disclosure of an individual's personal data for the purposes of the other organisations within the corporate group.[23]

Purpose limitation[24]

Organisations are limited to collecting, using or disclosing personal data for purposes that a reasonable person would consider appropriate in the circumstances and for a purpose to which the individual has consented.

20 Section 4(6)(b) of the PDPA.

21 Sections 13 to 17 of the PDPA.

22 In Section 12.42 of the PDPA Key Concepts Guidelines, the PDPA would consider a withdrawal notice of at least 10 business days from the day on which the organisation receives the withdrawal notice to be reasonable notice. Should an organisation require more time to give effect to a withdrawal notice, it is good practice for the organisation to inform the individual of the time frame under which the withdrawal of consent will take effect.

23 Section 12.32, PDPA Key Concepts Guidelines.

24 Section 18 of the PDPA.

Notification[25]

Organisations are obliged to notify individuals of their purposes for the collection, use and disclosure of the personal data on or before the collection. The PDPC has also released a guide to notification to assist organisations in providing clearer notifications to consumers on the collection, use and disclosure of personal data that includes suggestions on the layout, language and placement of notifications.[26]

Access and correction[27]

Save for certain exceptions, an organisation must, upon request, provide the individual with his or her personal data that the organisation has in its possession or control, and how the said personal data has been or may have been used or disclosed by the organisation during the past year. The organisation may charge a reasonable fee in responding to the access request.

The organisation is also obliged to allow an individual to correct an error or omission in his or her personal data upon request, unless the organisation is satisfied that there are reasonable grounds to deny such a request.[28]

An organisation should respond to an access or correction request within 30 days, beyond which the organisation should inform the individual in writing of the time frame in which it is able to provide a response to the request.[29]

Accuracy[30]

An organisation is obliged to make a reasonable effort to ensure that the personal data collected by or on behalf of the organisation is accurate and complete if they are likely to be used to make a decision that affects an individual or are likely to be disclosed to another organisation.

Protection[31]

An organisation is obliged to implement reasonable and appropriate security safeguards to protect the personal data in its possession or under its control from unauthorised access or similar risks. As a matter of good practice, organisations are advised to design and organise their security arrangements in accordance with the nature and varying levels of sensitivity of the personal data.[32]

Retention limitation[33]

An organisation may not retain the personal data for longer than is reasonable for the purpose for which they were collected, and for no longer than is necessary in respect of its business or legal purposes. Beyond that retention period, organisations should either delete or anonymise their records.

25 Section 20 of the PDPA.

26 PDPC Guide to Notification, issued on 11 September 2014 and revised on 26 September 2019.

27 Sections 21 and 22 of the PDPA.

28 Section 22(6) and Sixth Schedule of the PDPA.

29 Section 15.18, PDPA Key Concepts Guidelines.

30 Section 23 of the PDPA.

31 Section 24 of the PDPA.

32 See discussion in Sections 17.1–17.3, PDPA Key Concepts Guidelines.

33 Section 25 of the PDPA.

Transfer limitation[34]

An organisation may not transfer personal data to a country or territory outside Singapore unless it has taken appropriate steps to ensure that the data protection provisions will be complied with, and that the overseas recipient is able to provide a standard of protection that is comparable to the protection under the PDPA (see Section IV).

Accountability[35]

Previously known as the 'Openness Obligation', under the 'Accountability Obligation', an organisation is taken to be responsible for personal data in its possession or under its control. To that end, it is obliged to designate one or more individuals to be responsible for ensuring the organisation's compliance with the PDPA, implement necessary policies and procedures in compliance with the PDPA, and to ensure that this information is available on request.

iii Technological innovation and privacy law

The PDPC considers that an IP address or a network identifier, such as an International Mobile Equipment Identity number, may not on its own be considered personal data as it simply identifies a particular networked device. However, where IP addresses are combined with other information such as cookies, individuals may be identified via their IP addresses, which would thus be considered personal data.

In relation to organisations collecting data points tied to a specific IP address, for example, to determine the number of unique visitors to a website, the PDPC takes the view that if the individual is not identifiable from the data collected, then the information collected would not be considered personal data. If, on the other hand, an organisation tracks a particular IP address and profiles the websites visited for a period such that the individual becomes identifiable, then the organisation would be found to have collected personal data.

Depending on the purpose for the use of cookies, the PDPA would apply only where cookies collect, use or disclose personal data. Thus, in respect of session cookies that only collect and store technical data, consent is not required.[36] Where cookies used for behavioural targeting involve the collection and use of personal data, the individual's consent is required.[37] Express consent may not be necessary in all cases; consent may be reflected when an individual has configured his or her browser setting to accept certain cookies but reject others.

If an organisation wishes to use cloud-based solutions that involve the transfer of personal data to another country, consent of the individual may be obtained pursuant to the organisation providing a written summary of the extent to which the transferred personal data will be protected to a standard comparable with the PDPA.[38] It is not clear how practicable this would be in practice; a cloud-computing service may adopt multi-tenancy and data commingling architecture to process data for multiple parties. That said, organisations may take various precautions such as opting for cloud providers with the ability to isolate and identify personal data for protection, and ensure they have established platforms with a robust security and governance framework.

34 Section 26 of the PDPA.

35 Sections 11 and 12 of the PDPA.

36 Sections 6.5–6.8, Advisory Guidelines on the PDPA for Selected Topics (PDPA Selected Topics Guidelines), issued on 24 September 2013 and revised on 9 October 2019.

37 Section 6.11, PDPA Selected Topics Guidelines.

38 Section 9(4)(a) of the Personal Data Protection Regulations 2014.

As regards social media, one issue arises where personal data are disclosed on social networking platforms and become publicly available. As noted earlier, the collection, use and disclosure of publicly available data is exempt from the requirement to obtain consent. If, however, the individual changes his or her privacy settings so that the personal information is no longer publicly available, the PDPC has adopted the position that, as long as the personal data in question were publicly available at the point of collection, the organisation will be able to use and disclose the same without consent.[39]

iv Specific regulatory areas

Minors

The PDPA does not contain special protection for minors (under 21 years of age).[40] However, the Selected Topics Advisory Guidelines note that a minor of 13 years or older typically has sufficient understanding to provide consent on his or her own behalf. Where a minor is below the age of 13, an organisation should obtain consent from the minor's parents or legal guardians on the minor's behalf.[41] The Education Guidelines[42] provide further guidance on when educational institutions seeking to collect, use or disclose personal data of minors are required to obtain the consent of the parent or legal guardian of the student.

Given the heightened sensitivity surrounding the treatment of minors, the PDPC recommends that organisations ought to take relevant precautions on this issue. Such precautions may include making the terms and conditions easy to understand for minors, placing additional safeguards in respect of personal data of minors and, where feasible, anonymising their personal data before use or disclosure.

Financial institutions

A series of notices issued by the Monetary Authority of Singapore (MAS),[43] the country's central bank and financial regulatory authority, require various financial institutions to, among other things:

a upon request, provide access as soon as reasonably practicable to personal data in the possession or under the control of the financial institution, which relates to an individual's factual identification data such as full name or alias, identification number, residential address, telephone number, date of birth and nationality; and

b correct an error or omission in relation to the categories of personal data set out above upon request by a customer if the financial institution is satisfied that the request is reasonable.

39 Section 12.61, PDPA Key Concepts Guidelines.

40 Section 7.1, PDPA Selected Topics Guidelines.

41 Section 14(4) of the PDPA. See also discussion at Section 7.9 of the PDPA Selected Topics Guidelines.

42 Sections 2.5–2.10, PDPC Advisory Guidelines on the Education Sector (the Education Guidelines), issued 11 September 2014 and revised on 31 August 2018.

43 MAS Notice SFA13-N01 regulating approved trustees; MAS Notice 626 regulating banks; MAS Notice SFA04-N02 regulating capital markets intermediaries; MAS Notice FAA-N06 regulating financial advisers; MAS Notice 824 regulating finance companies; MAS Notice 3001 regulating holders of money-changers' licences and remittance licences; MAS Notice PSOA-N02 regulating holders of stored value facilities; MAS Notice 314 regulating life insurers; MAS Notice 1014 regulating merchant banks; and MAS Notice TCA-N03 regulating trust companies.

On 5 December 2019, the MAS issued two further Notices: a Notice on Cyber Hygiene[44] to licensees and operators of designated payment systems and a Notice on Technology Risk Management[45] to operators and settlement institutions of designated payment systems, pursuant to Section 102(1) of the Payment Services Act 2019. They set out, among other things, cybersecurity requirements to protect customer information from unauthorised access or disclosure.

In addition, legislative changes to the Monetary Authority of Singapore Act, aimed at enhancing the effectiveness of the anti-money laundering and the countering of financing of terrorism (AML/CFT) regime of the financial industry in Singapore, came into force on 26 June 2015.

Following the changes, MAS now has the power to share information on financial institutions with its foreign counterparts under their home jurisdiction on AML/CFT issues. MAS may also make AML/CFT supervisory enquiries on behalf of its foreign counterparts. Nonetheless, strong safeguards are in place to prevent abuse and 'fishing expeditions'. In granting requests for information, MAS will only provide assistance for bona fide requests. Any information shared will be proportionate to the specified purpose, and the foreign AML/CFT authority has to undertake not to use the information for any purpose other than the specified purpose, and to maintain the confidentiality of any information obtained.

Electronic marketing

The PDPA contains provisions regarding the establishment of a national DNC Registry and obligations for organisations that send certain kinds of marketing messages to Singapore telephone numbers to comply with these provisions. The PDPA Healthcare Guidelines[46] provide further instructions on how the DNC provisions apply to that sector, particularly in relation to the marketing of drugs to patients. In relation to the DNC Registry, the obligations only apply to senders of messages or calls to Singapore numbers, and where the sender is in Singapore when the messages or calls are made, or where the recipient accesses them in Singapore. Where there is a failure to comply with the DNC provisions, fines of up to S$10,000 may be imposed for each offence.

Employees

The PDPC provides that organisations should inform employees of the purposes of the collection, use and disclosure of their personal data and obtain their consent.

Employers are not required to obtain employee consent in certain instances. For instance, the collection of employee's personal data for the purpose of managing or terminating the employment relationship does not require the employee's consent, although employers are still required to notify their employees of the purposes for their collection, use and disclosure.[47] Examples of managing or terminating an employment relationship can include using the employee's bank account details to issue salaries or monitoring how the employee uses company computer network resources. The PDPA does not prescribe the

44 MAS Notice PSN06.

45 MAS Notice PSN05.

46 Section 6 of the Advisory Guidelines for the Healthcare Sector (PDPC Healthcare Guidelines), issued on 11 September 2014 and revised on 28 March 2017.

47 Paragraph 1(o) Second Schedule, Paragraph 1(j) Third Schedule, and Paragraph 1(s) Fourth Schedule of the PDPA.

manner in which employees may be notified of the purposes of the use of their personal data; as such, organisations may decide to inform their employees of these purposes via employment contracts, handbooks or notices on the company intranet.

In addition, collection of employee personal data necessary for 'evaluative purposes', such as to determine the suitability of an individual for employment, neither requires the potential employee to consent to, nor to be notified of, their collection, use or disclosure.[48] Other legal obligations, such as to protect confidential information of their employees, will nevertheless continue to apply.[49]

Section 25 of the PDPA requires an organisation to cease to retain or anonymise documents relating to the personal data of an employee once the retention is no longer necessary.

IV PDPA AND INTERNATIONAL DATA TRANSFER

An organisation may only transfer personal data outside Singapore subject to requirements prescribed under the PDPA so as to ensure that the transferred personal data is afforded a standard of protection comparable to the PDPA.[50]

An organisation may transfer personal data overseas if it has taken appropriate steps to ensure that:

a it will comply with the data protection provisions while the personal data remains in its possession or control; and

b the recipient is bound by legally enforceable obligations to protect the personal data in accordance with standards comparable to the PDPA.[51] Such legally enforceable obligations would include any applicable laws of the country to which the personal data is transferred, contractual obligations or binding corporate rules for intra-company transfers.[52]

Notwithstanding the above, an organisation is taken to have satisfied the latter requirement if, inter alia, the individual consents to the transfer pursuant to the organisation providing a summary in writing of the extent to which the personal data transferred to another country will be protected to a standard comparable to the PDPA;[53] or where the transfer is necessary for the performance of a contract. Alternatively, if an overseas recipient is APEC CBPR certified or APEC PRP certified (where the recipient is a data intermediary), the recipient will be taken to be bound by legally enforceable obligations to provide a standard of protection that is at least comparable to the PDPA.[54]

48 Paragraph 1(f) Second Schedule, Paragraph 1(f) Third Schedule and Paragraph 1(h) Fourth Schedule of the PDPA.

49 Sections 5.14–5.16 of the PDPA Selected Topics Guidelines.

50 Section 26(1) of the PDPA. The conditions for the transfer of personal data overseas are specified within the Personal Data Protection Regulations 2014 (PDP Regulations).

51 Regulation 9 of the PDP Regulations.

52 Regulation 10 of the PDP Regulations.

53 Regulations 9(3)(a) and 9(4)(a) of the PDP Regulations.

54 Regulation 10A of the PDP Regulations

In respect of personal data that simply passes through servers in Singapore en route to an overseas destination, the transferring organisation will be deemed to have complied with the transfer limitation obligation.[55]

The PDPA Key Concepts Guidelines also provide examples to illustrate situations in which organisations are deemed to have transferred personal data overseas in compliance with their transfer limitation obligation pursuant to Section 26 of the PDPA, regardless of whether the foreign jurisdiction's privacy laws are comparable to the PDPA. An example is when a tour agency needs to share a customer's details (e.g., his or her name and passport number) to make hotel and flight bookings. The tour agency is deemed to have complied with Section 26 since the transfer is necessary for the performance of the contract between the agency and the customer.[56]

An organisation is also deemed to have complied with the transfer limitation obligation if the transfer is necessary for the performance of a contract between a Singaporean company and a foreign business, and the contract is one that a reasonable person would consider to be in the individual's interest.[57]

Other examples given by the PDPA Key Concepts Guidelines include the transferring of publicly available personal data, and transferring a patient's medical records to another hospital where the disclosure is necessary to respond to a medical emergency.

The PDPA Key Concepts Guidelines also sets out the scope of contractual clauses at Section 19.7 for recipients to comply with the required standard of protection in relation to personal data received so that it is comparable to the protection under the PDPA. The PDPA Key Concepts Guidelines sets out in a table (reproduced below) the areas of protection a transferring organisation should minimally set out in its contract in two situations: where the recipient is another organisation (except a data intermediary); and where the recipient is a data intermediary (i.e., an organisation that processes the personal data on behalf of the transferring organisation pursuant to a contract).

S/N	Area of protection	Recipient is:	
		Data intermediary	Organisation (except data intermediary)
1	Purpose of collection, use and disclosure by recipient	–	Yes
2	Accuracy	–	Yes
3	Protection	Yes	Yes
4	Retention limitation	Yes	Yes
5	Policies on personal data protection	–	Yes
6	Access	–	Yes
7	Correction	–	Yes

55 Regulation 9(2)(a) of the PDP Regulations.

56 Section 19.6 of the PDPA Key Concepts Guidelines.

57 Section 9(3)(d) of the PDP Regulations.

V PDPA AND COMPANY POLICIES AND PRACTICES

Organisations are obliged to develop and implement policies and practices necessary to meet their obligations under the PDPA.[58] Organisations must also develop a complaints mechanism,[59] and communicate to their staff the policies and practices they have implemented.[60] Information on policies and practices, including the complaints mechanism, is to be made available on request.[61] Every organisation is also obliged to appoint a data protection officer, who would be responsible for ensuring the organisation's compliance with the PDPA, and to make the data protection officer's business contact information publicly available.[62]

As a matter of best practice, an organisation should have in place notices and policies that are clear, easily accessible and comprehensible. Some of the policies and processes that an organisation may consider having in place are set out below.

i Data protection policy

If an organisation intends to collect personal data from individuals, it would be required to notify them of the purposes for the collection, use and disclosure of the personal data and seek consent before collecting the personal data. It should also state whether the personal data will be disclosed to third parties, and if so, who these organisations are. Further, where it is contemplated that the personal data may be transferred overseas, the organisation should disclose this and provide a summary of the extent to which the personal data would receive protection comparable to that under the PDPA, so that it may obtain consent from the individual for the transfer. The data protection policy may also specify how requests to access and correct the personal data may be made. To satisfy the requirement in the PDPA that data protection policies are available on request, the organisation may wish to make its policy available online.

ii Cookie policy

If the corporate website requires collection of personal data or uses cookies that require collection of personal data, users ought to be notified of the purpose for the collection, use or disclosure of the personal data, and prompted for their consent in that regard.

iii Complaints mechanism

The organisation should develop a process to receive and respond to complaints it receives, and such process should be made available to the public on request.

iv Contracts with data intermediaries

Contracts with data intermediaries should set out clearly the intermediaries' obligations, and include clauses relating to the retention period of the data and subsequent deletion or destruction, security arrangements, access and correction procedures, and audit rights of

58 Section 12(a) of the PDPA.
59 Section 12(b) of the PDPA.
60 Section 12(c) of the PDPA.
61 Section 12(d) of the PDPA.
62 Sections 11(4), 11(5) of the PDPA.

the organisation over the data intermediaries. Where a third party is engaged to collect data on an organisation's behalf, the contract should specify that the collection is conducted in compliance with the data protection provisions.

v Employee data protection policy

Employees should be notified of how their personal data may be collected, used or disclosed. The mode of notification is not prescribed, and the employer may choose to inform the employee of these purposes via employment contracts, handbooks or notices on the company intranet. Consent is not required if the purpose is to manage or terminate the employment relationship; as an example, the company should notify employees that it may monitor network activities, including company emails, in the event of an audit or review.

vi Retention and security of personal data

Organisations should ensure that there are policies and processes in place to ensure that personal data are not kept longer than is necessary, and that there are adequate security measures in place to safeguard the personal data. An incident-response plan should also be created to ensure prompt responses to security breaches.

VI PDPA AND DISCOVERY AND DISCLOSURE

The data protection provisions under the PDPA do not affect any rights or obligations under other laws.[63] As such, where the law mandates disclosure of information that may include personal data, another law would prevail to the extent that it is inconsistent with the PDPA. For instance, the Prevention of Corruption Act imposes a legal duty on a person to disclose any information requested by the authorities. Under those circumstances, the legal obligation to disclose information would prevail over the data protection provisions.

The PDPA has carved out specific exceptions in respect of investigations and proceedings. Thus, an organisation may collect data about an individual without his or her consent where the collection is necessary for any investigation or proceedings, so as not to compromise the availability or accuracy of the personal data.[64] Further, an organisation may use personal data about an individual without the consent of the individual if the use is necessary for any investigation or proceedings.[65] These exceptions, however, do not extend to internal audits or investigations. Nevertheless, it may be argued that consent from employees is not required as such audits would fall within the purpose of managing or terminating the employment relationship.[66] Employees may be notified of such potential purposes of use of their personal data in their employee handbooks or contracts, as the case may be.

On an international scale, Singapore is active in providing legal assistance and in the sharing of information, particularly in respect of criminal matters. That said, the PDPC may not share any information with a foreign data protection body unless there is an undertaking

63 Section 4(6) of the PDPA.

64 Second Schedule, Paragraph 1(e) of the PDPA.

65 Third Schedule, Paragraph 1(e) of the PDPA.

66 As discussed earlier, consent is not required if the purpose for the collection, use and disclosure of personal data is for managing or terminating the employment relationship.

in writing that it will comply with its terms in respect of the disclosed data. This obligation is mutual, and the PDPA also authorises the PDPC to enter into a similar undertaking required for a foreign data protection body where required.[67]

VII PDPA PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

The PDPC is the key agency responsible for administering and enforcing the PDPA. Its role includes, inter alia, reviewing complaints from individuals,[68] carrying out investigations (whether on its own accord or upon a complaint), and prosecuting and adjudicating on certain matters arising out of the PDPA.[69]

To enable the PDPC to carry out its functions effectively, it has been entrusted with broad powers of investigation,[70] including the power to require organisations to produce documents or information, and the power to enter premises with or without a warrant to carry out a search. In certain circumstances, the PDPC may obtain a search and seizure order from the state courts to search premises and take possession of any material that appears to be relevant to an investigation.

Where the PDPC is satisfied that there is non-compliance with the data protection provisions, it may issue directions to the infringing organisation to rectify the breach and impose financial penalties up to S$1 million.[71] The PDPC may also in its discretion compound the offence.[72] Certain breaches can attract penalties of up to three years' imprisonment.[73] In addition to corporate liability, the PDPA may also hold an officer of the company to be individually accountable if the offence was committed with his or her consent or connivance, or is attributable to his or her neglect.[74] Further, employers are deemed to be vicariously liable for the acts of their employees, unless there is evidence showing that the employer had taken steps to prevent the employee from engaging in the infringing acts.[75]

Directions issued by the PDPC may be appealed to be heard before the Appeal Committee. Thereafter, any appeals against decisions of the Appeal Committee shall lie to the High Court, but only on a point of law or the quantum of the financial penalty. There would be a further right of appeal from the High Court's decisions to the Court of Appeal, as in the case of the exercise of its original civil jurisdiction.[76]

In relation to breaches of the DNC Registry provisions, an organisation may be liable for fines of up to S$10,000 for each breach.

67 Section 10(4) of the PDPA.

68 Section 28 of the PDPA.

69 See Sections 28(2) and 29(1) of the PDPA. The PDPC has the power to give directions in relation to review applications made by complainants and contraventions to Parts III to VI of the PDPA.

70 Section 50 of the PDPA. See also Ninth Schedule of the PDPA.

71 Section 29 of the PDPA.

72 Section 55 of the PDPA.

73 Section 56 of the PDPA.

74 Section 52 of the PDPA.

75 Section 53 of the PDPA.

76 Section 35 of the PDPA.

ii Recent enforcement cases

The PDPC published 51 enforcement decisions in 2019, and 17 decisions from January 2020 to June 2020. In the decisions, the PDPC provides substantial factual detail and legal reasoning, and the decisions are another source of information for companies seeking guidance on particular issues.

Several enforcement actions in 2019 and the first half of 2020 set out the PDPC's typical mix of behaviour remedies combined with financial penalties, including the following.

Amicus Solutions Pte Ltd and Mr Ivan Chua (August 2019)[77]

The PDPC issued a fine of S$48,000 to Amicus Solutions and S$10,000 to Chua, a financial adviser director, for Amicus Solutions' failure to notify and obtain consent to disclose personal data that it sold to Chua, who used the personal data for telemarketing purposes without obtaining consent.

Ninja Logistics Pte Ltd (November 2019)[78]

The PDPC imposed directions and a financial penalty of S$90,000 on the organisation, for its failure to put in place reasonable security arrangements to protect customers' data in relation to the Tracking Function Page on its website, which resulted in customers' data being publicly accessible.

Henry Park Primary School Parents' Association (February 2020)[79]

PDPC found that the organisation failed to put in place reasonable security measures to protect its members' personal data, did not appoint a DPO, and did not have written policies and practices necessary to ensure compliance with the PDPA. The PDPC did not issue a fine, as it took into consideration that the organisation was a volunteer organisation primarily made up of parents, but directed that it take certain measures including appointing a DPO and implementing data protection policies and training.

iii Private litigation

Anyone who has suffered loss or damage directly arising from a contravention of the data protection provisions may obtain an injunction, declaration, damages or any other relief against the errant organisation in civil proceedings in court. However, if the PDPC has made a decision in respect of a contravention of the PDPA, no private action against the organisation may be taken for that contravention until after the right of appeal has been exhausted and the final decision is made.[80] Once the final decision is made, a person who suffers loss or damage as a result of a contravention of the PDPA may commence civil proceedings directly.[81]

77 Decision Citation: [2019] SGPDPC 33.

78 Decision Citation: [2019] SGPDPC 39.

79 Case No. DP-1903-B3531

80 Section 32 of the PDPA.

81 Advisory Guidelines on Enforcement of the Data Protection Provisions issued by the PDPC on 21 April 2016 at Paragraph 34.3.

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

The PDPA applies to foreign organisations in respect of activities relating to the collection, use and disclosure of personal data in Singapore regardless of their physical presence in Singapore.

Thus, where foreign organisations transfer personal data into Singapore, the data protection provisions would apply in respect of activities involving personal data in Singapore. These obligations imposed under the PDPA may be in addition to any applicable laws in respect of the data activities involving personal data transferred overseas.

IX CYBERSECURITY AND DATA BREACHES

i Data breaches

While the PDPA obliges organisations to protect personal data, it does not currently require organisations to notify authorities in the event of a data breach. However, as noted below, there are proposals to amend the PDPA to introduce a mandatory data breach reporting requirement. In the absence of mandatory data breach requirements, government sector regulators have imposed certain industry-specific reporting obligations. For example, MAS issued a set of notices to financial institutions on 1 July 2014 to direct that all security breaches should be reported to MAS within one hour of discovery.

ii Cybersecurity

Singapore is not a signatory to the Council of Europe's Convention on Cybercrime.

In Singapore, the CMA and the Cybersecurity Act are the key legislations governing cybercrime and cybersecurity. The CMA is primarily focused on defining various cybercrime offences, including criminalising the unauthorised accessing[82] or modification of computer material,[83] use or interception of a computer service,[84] obstruction of use of a computer,[85] and unauthorised disclosure of access codes.[86]

The 2017 amendments to the CMA added the offences of obtaining or making available personal information that the offender believes was obtained through a computer crime[87] and using or supplying software or other items to commit or facilitate the commission of a computer crime.[88]

The Cybersecurity Act greatly expands national cybersecurity protections, including by imposing affirmative reporting, auditing and other obligations on CII owners and by appointing a new Commissioner of Cybersecurity with broad authority, including the power to establish mandatory codes of practice and standards of performance for CII owners.

Under Section 2 of the Cybersecurity Act, 'cybersecurity' is defined as the state in which a computer or system is protected from unauthorised access or attack and, because of that state:

82 Sections 3 and 4 of the CMA.
83 Section 5 of the CMA.
84 Section 6 of the CMA.
85 Section 7 of the CMA.
86 Section 8 of the CMA.
87 Section 8A of the CMA.
88 Section 8B of the CMA.

a the computer or system continued to be available and operational;
b the integrity of the computer or system is maintained; or
c the integrity and confidentiality of information stored in, processed by or transmitted through the computer or system is maintained.

CII is defined as computer systems, located at least partly within Singapore, that are necessary for the continuous delivery of an essential service such that the loss of a system would have a debilitating effect on the availability of the essential service in Singapore. The Commissioner will designate those systems that it determines qualify as CII, and will notify the legal owner of such systems in writing. An owner or operator of a system that has been designated as CII must comply with various requirements set forth in the Act, including but not limited to reporting to the Commissioner certain prescribed incidents, establishing mechanisms and processes for detecting cybersecurity threats and incidents, reporting any material changes to the design, configuration, security or operation of the CII, complying with all codes of practice and standards of performance issued by the Commissioner, conducting regular audits of compliance of the CII with the Cybersecurity Act, and participating in cybersecurity exercises as required by the Commissioner.

Under the Cybersecurity Act, however, the Commissioner's authority goes beyond CII. Any organisation, even if it does not own or operate CII, must cooperate with the Commissioner in the investigation of cybersecurity threats and incidents. In furtherance of such investigations, the Commissioner may, among other things, require any person to produce any physical or electronic record or document, and require an organisation to carry out such remedial measures or cease carrying out such activities as the Commissioner may direct. Finally, the Act establishes a licensing regime for providers of (1) services that monitor the cybersecurity levels of other persons' computers or systems; and (2) services that assess, test or evaluate the cybersecurity level of other persons' computers or systems by searching for vulnerabilities in, and compromising, the defences of such systems. Any person who provides a licensable cybersecurity service without a licence will be guilty of an offence.

The Cybersecurity Act represents a move away from sector-based regulation. The Act requires mandatory reporting to the new Commissioner of Cybersecurity of 'any cybersecurity incident' (which is broader than but presumably would also include data breaches) that relates to CII or systems connected with CII. In issuing the bill, the government noted that it had considered sector-based cybersecurity legislation but had concluded that an omnibus law that would establish a common and consistent national framework was the better option. However, sectorial regulators continue to play a part in regulation in this area. For example, in December 2018, MAS launched a S$30 million Cybersecurity Capabilities Grant to enhance cybersecurity capabilities in the financial sector and assist financial institutions in developing local talent in the cybersecurity sector. The IMDA has also formulated Codes of Practice to enhance the cybersecurity preparedness for designated licensees. The Codes are currently imposed on major Internet Service Providers in Singapore for mandatory compliance.

X OUTLOOK

In keeping with its declared strategy, Singapore continues to clarify and enforce its existing data privacy and cybersecurity regime, and future legislative developments appear forthcoming.

From 14 to 28 May 2020, the Ministry of Communications and Information and the PDPC launched a public consultation on proposed amendments to the PDPA and related amendments to the SCA. Notable proposals include:

a the introduction of a mandatory breach notification requirement if a data breach results in, or is likely to result in, significant harm to individuals, or is of a significant scale;

b the expansion of the definition of 'deemed consent' to allow greater scope for organisations to collect, use or disclose personal data;

c the introduction of a 'Legitimate Interests Exception' and a 'Business Improvement Exception' to allow organisations to collect, use or disclose personal data without consent in a wider array of circumstances;

d the introduction of a data portability obligation to give individuals greater choice and control in transferring their data to other organisations;

e the introduction of new offences relating to egregious mishandling of personal data; and

f heavier financial penalties for non-compliance with the PDPA (up to 10 per cent of an organisation's annual gross turnover in Singapore or S$1 million, whichever is higher).

These amendments appear designed to align Singapore's existing data protection regime with international developments, with the aim of strengthening public trust and enhancing organisational accountability.

Appendix 1

ABOUT THE AUTHORS

YUET MING THAM

Sidley Austin LLP

Yuet Ming Tham is the global co-leader of the white collar: government litigation and investigations practice and leader of the Asia Pacific Compliance and Investigations practice. Yuet is also Asia Pacific Chair of the firm's Diversity and Inclusion Committee. She speaks fluent English, Mandarin, Cantonese and Malay and is admitted in New York, England & Wales, Hong Kong and Singapore.

Yuet focuses on cross-border compliance and investigations, and advises international corporations on cybersecurity and privacy.

Yuet was most recently awarded 'Top 100 Women in Law' in the Asia Pacific region 2020 and 'Dispute Resolution Star: White-collar' in 2019 by *Benchmark Litigation Asia-Pacific* and recognised in *Who's Who Legal: Thought Leaders – Global Investigations Review* 2019/2020 and *Who's Who Legal: Thought Leaders – Hong Kong* 2020. Yuet has also been awarded the Emerging Markets 'Compliance and Investigations Lawyer of the Year' by *The American Lawyer*, with the team also recognised as the 'Compliance/Investigations Firm of the Year'.

She has also been acknowledged as a 'Leading Lawyer' by *Chambers Asia-Pacific* across four categories namely 'Dispute Resolution: Litigation', 'Corporate Investigations/ Anti-Corruption', 'Life Sciences' and 'Financial Services: Contentious Regulatory'. Additionally, Yuet is recognised in the 'Financial Services Regulatory' in *IFLR1000* as a 'Leading Lawyer' and has also been listed by *Who's Who Legal* as a 'Leading Business Lawyer' in three separate categories, namely 'Life Sciences', 'Business Crime Defence' and 'Investigations'. She is regarded as 'one of the best-informed regulatory lawyers in the region' and was the only lawyer awarded the Client Choice Award 2016 by the *International Law Office* in the White Collar Crime practice in Hong Kong. In the 2018 edition of *Chambers Global and Chambers Asia-Pacific*, under the Corporate Investigations chapter, Yuet is described as 'exceptionally bright' and 'very responsive and knowledgeable and can immediately dive into the issues'. According to the 2015 edition of *Chambers Global,* 'Ms. Tham is described by clients as "a marvelous and gifted attorney" while peers acknowledge her prowess in working with clients in the life science sector. She is active advising on anti-corruption issues across Asia, with a focus on assisting businesses on FCPA investigations in China, Japan, South Korea, Indonesia and Vietnam.' Meanwhile, *Chambers Asia Pacific* noted that Yuet 'is frequently sought after by international corporations, who respect her experience and expertise in risk management.'

SIDLEY AUSTIN LLP

39/F Two International Finance Centre
Central
Hong Kong
Tel: +852 2509 7645
Fax: +852 2509 3110
yuetming.tham@sidley.com
www.sidley.com

an LBR business

ISBN 978-1-83862-485-9