THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

FIFTH EDITION

Editor
Alan Charles Raul

THE LAWREVIEWS

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

Fifth Edition

Reproduced with permission from Law Business Research Ltd
This article was first published in October 2018
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 MANAGERS
Thomas Lee, Joel Woods

SENIOR ACCOUNT MANAGER
Pere Aspinall

ACCOUNT MANAGERS
Jack Bagnall, Sophie Emberson, Katie Hodgetts

PRODUCT MARKETING EXECUTIVE
Rebecca Mogridge

RESEARCHER
Keavy Hunnigal-Gaw

EDITORIAL COORDINATOR
Thomas Lawson

HEAD OF PRODUCTION
Adam Myers

PRODUCTION EDITOR
Anna Andreoli

SUBEDITOR
Martin Roach

CHIEF EXECUTIVE OFFICER
Paul Howarth

Published in the United Kingdom
by Law Business Research Ltd, London
87 Lancaster Road, London, W11 1QQ, UK

www.TheLawReviews.co.uk

ISBN 978-1-912228-62-1

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

ACKNOWLEDGEMENTS

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

ALLENS

ASTREA

BOGSCH & PARTNERS LAW FIRM

BTS&PARTNERS

JUN HE LLP

KOBYLAŃSKA & LEWOSZEWSKI KANCELARIA PRAWNA SP J

M&M BOMCHIL

MÁRQUEZ, BARRERA, CASTAÑEDA & RAMÍREZ

MATHESON

MATTOS FILHO, VEIGA FILHO, MARREY JR E QUIROGA ADVOGADOS

NNOVATION LLP

NOERR

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SK CHAMBERS

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

WALDER WYSS LTD

WINHELLER RECHTSANWALTSGESELLSCHAFT MBH

CONTENTS

Chapter 21

SINGAPORE

Yuet Ming Tham[1]

I OVERVIEW

In 2017 and 2018, Singapore has continued to rapidly develop its data protection, cybercrime, and cybersecurity regimes. As set out in Singapore's October 2016 cybersecurity strategy report,[2] the government views its efforts in these areas as part of an integrated cybersecurity plan to protect the country from cyberthreats and to reinforce Singapore's standing as a leading information systems hub. 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 and Cybersecurity Act (CMCA) to combat cybercrime and other cyberthreats, and the recently passed Cybersecurity Act (the Cybersecurity Act), which focuses on protecting Singapore's critical information infrastructure (CII) and establishing a comprehensive national cybersecurity framework.

In this chapter, we will outline the key aspects of the PDPA, CMCA 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.

This chapter also will review the amendments to the CMCA and the CMCA's linkages with the Cybersecurity Act. The discussion will cover the proposed consolidation of cybersecurity authority within Singapore's Cybersecurity Agency (CSA) and the new position of Commissioner of Cybersecurity established by the Cybersecurity Act.

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 – in the 12 months from September 2017 to August 2018. In July 2017, the PDPC had initiated a public consultation to consider proposed changes to the PDPA that would have the effect of

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

2 See Singapore's Cybersecurity Strategy, Cybersecurity Agency of Singapore (October 2016) (Cybersecurity Report).

(1) broadening the circumstances under which organisations could collect, use and disclose personal data without consent, and (2) imposing a mandatory data breach notification requirement in certain situations. The consultation period closed on 5 October 2017, and the PDPC issued its responses to the feedback on 1 February 2018.[3] Regarding consent, the PDPC had proposed not requiring consent if it would be impractical for the organisation to obtain consent and the collection, use and disclosure of the personal data were not expected in any way to have an adverse effect on the individual. In such a situation, the PDPC proposed allowing a notification-of-purpose in lieu of consent. In response to public feedback, the PDPC decided to remove the condition of 'impractical to obtain consent.' The PDPC also proposed creating a catch-all 'legal or business purpose' exception to consent where it would not be desirable or appropriate to obtain the individual's consent and the benefits to the public generally or to a subset of the public 'clearly outweigh' any adverse effect or risks to the individual (such as where an organisation would like to share personal data in order to detect and prevent fraudulent activity). Following public feedback, the PDPC proposed to instead provide for a 'legitimate interests' exception to consent, which would be an evolution of the 'legal or business purpose' approach and would be further clarified in future guidelines from the PDPC. Regarding the data breach notification requirement, the PDPC had proposed to require data breach notification in the following circumstances: (1) if there is any risk of impact or harm to affected individuals, the organisation must notify the individuals and the PDPC; (2) if the scale of the data breach is 'significant' (i.e., involving 500 or more individuals), the organisation must notify the PDPC; and (3) if a data intermediary experiences a breach, it must notify its clients immediately. In response to public feedback, the PDPC announced that it will not prescribe a statutory threshold for the number of affected individuals (i.e., 500) that would constitute a 'significant' data breach, but rather would issue guidance on assessing the scale of impact.

In March 2018, Singapore announced that it had joined the Asia-Pacific Economic Cooperation (APAC) Cross-Border Privacy Rules (CBPR) system, as well as the APAC Privacy Recognition for Processors (PRP) programme. Upon joining, Singapore became the sixth member of the CBPR system – which already included Canada, Japan, Korea, Mexico and the United States – and the second member of the PRP programme after the United States. APEC established the CBPR programme to facilitate the transmittal of personal data across national borders within and between companies and organisations. (The APEC PRP programme seeks to accomplish similar goals for data processors.) Companies and organisations in CBPR member countries that collect and use personal data may obtain CBPR certification through a compliance review process by an independent evaluator. The Singapore government has indicated that the PDPC intends to launch a certification scheme for both the CBPR and PRP standards by the end of 2018.

In April 2018, the PDPC issued a Public Consultation for Managing Unsolicited Commercial Messages and the Provision of Guidance to Support Innovation in the Digital Economy. This consultation aims to bring together and streamline existing 'do not call' rules contained in the PDPA and the Spam Control Act, ban parties from screening the do not call registry and selling the resulting information to marketers, and include instant messages within the remit of the PDPA. This consultation closed on 12 June 2018.

3 www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Legislation-and-Guidelines/PDPC-Response-to-Feedback-for-Public-Consultation-on-Approaches-to-Managing-Personal-Data-in-the-Dig.pdf.

ii CMCA developments and the Cybersecurity Act

The CMCA and the Cybersecurity Act are closely linked. In the October 2016 Cybersecurity Report, the government noted the need for a comprehensive framework to prevent and manage the increasingly sophisticated threats to Singapore's cybersecurity. According to the report, the Cybersecurity Act would establish that framework and would complement the existing cybercrime measures set out in the CMCA.

In 2013, the government amended the existing Computer Misuse Act, renaming it the Computer Misuse and Cybersecurity Act, to strengthen the country's response to national-level cyberthreats. In 2017, the government introduced further amendments to the CMCA, and the amended law came into effect on 1 June 2017. The amendments broadened the scope of the CMCA by criminalising certain conduct not already covered by the existing law and enhancing penalties in certain situations. For example, the new provisions of the CMCA criminalise 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 CMCA 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, on 5 February 2018, Singapore passed the Cybersecurity Bill No. 2/2018 (the Cybersecurity Act), a draft of which had previously been issued for public consultation on 10 July 2017. The Cybersecurity Act addresses the regulation of CII, creates a new Commissioner of Cybersecurity with significant powers to prevent and respond to cybersecurity incidents in Singapore, and sets up a licensing scheme for providers of certain cybersecurity services.

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 reporting to the Commissioner certain prescribed incidents, establishing mechanisms and processes for detecting cybersecurity threats and incidents, and reporting any material changes to the design, configuration, security or operation of the CII.

Under the Cybersecurity Act, the Commissioner's authority goes beyond CII, however. 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. According to the Cybersecurity Agency's 'Cybersecurity FAQs', the licensing framework is expected to be implemented in the second half of 2019.[4]

iii 2018 Developments and regulatory compliance

Although the developments with the CMCA 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 CMCA is primarily a criminal statute, and the government has not issued any regulations or guidelines for the CMCA. 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.[5]

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.

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.[6] 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.[7] There are certain exceptions to which the PDPA would apply. Business contact information of an individual generally falls outside the ambit of the PDPA,[8] as does personal data that is publicly available.[9] In addition, personal data of an individual who has been deceased for over 10 years[10] and personal data contained within records for over 100 years is exempt.[11]

4 www.csa.gov.sg/~/media/csa/cybersecurity_bill/cybersecurity%20act%20-%20faqs.pdf.

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

6 Section 2 of the PDPA.

7 Section 5.30, PDPA Key Concepts Guidelines.

8 Section 4(5) of the PDPA.

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

10 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.

11 Section 4(4) of the PDPA.

Pursuant to the PDPA, organisations are responsible for personal data in their possession or under their control.[12] 'Organisations' include individuals who are resident in Singapore, local and foreign companies, associations and bodies (incorporated and unincorporated), whether or not they have an office or a place of business in Singapore.[13] The PDPA does not apply to public agencies.[14] 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.[15]

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 its services remains fully responsible in respect of the data as if it had processed the data on its own.[16]

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.[17]

Subsidiary legislation to the PDPA includes implementing regulations relating to the Do Not Call (DNC) Registry,[18] enforcement,[19] composition of offences,[20] requests for access to and correction of personal data, and the transfer of personal data outside Singapore.[21]

There is also various 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.[22]

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.

12 Section 11(2) of the PDPA.
13 Section 2 of the PDPA.
14 Section 4(1)(c) of the PDPA.
15 Section 4(1)(a) and (b) of the PDPA.
16 Section 4(3) of the PDPA.
17 Section 32 of the PDPA.
18 Personal Data Protection (Do Not Call Registry) Regulations 2013.
19 Personal Data Protection (Enforcement) Regulations 2014.
20 Personal Data Protection (Composition of Offences) Regulations 2013.
21 Personal Data Protection Regulations 2014.
22 Section 6 of the PDPA.

Consent[23]

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.[24] 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.[25]

Purpose limitation[26]

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.

Notification[27]

Organisations are obliged to notify individuals of their purposes for the collection, use and disclosure of the personal data on or before the collection, use and disclosure. 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.[28]

Access and correction[29]

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.[30]

---

23 Sections 13 to 17 of the PDPA.

24 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.

25 Section 12.32, PDPA Key Concepts Guidelines.

26 Section 18 of the PDPA.

27 Section 20 of the PDPA.

28 PDPC Guide to Notification, issued on 11 September 2014.

29 Sections 21 and 22 of the PDPA.

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

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.[31]

Accuracy[32]

An organisation is obliged to make a reasonable effort to ensure that the personal data collected by or on behalf of the organisation are 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[33]

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.[34]

Retention limitation[35]

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 purpose. Beyond that retention period, organisations should either delete or anonymise their records.

Transfer limitation[36]

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).

Openness[37]

An organisation is obliged to implement necessary policies and procedures in compliance with the PDPA, and to ensure that this information is available publicly.

iii Technological innovation and privacy law

The PDPC considers that an IP address or network identifier, such as an International Mobile Equipment Identity number, may not on its own be considered personal data as it simply

31 15.18, PDPA Key Concepts Guidelines.
32 Section 23 of the PDPA.
33 Section 24 of the PDPA.
34 See discussion in Sections 17.1–17.3, PDPC Key Concepts Guidelines.
35 Section 25 of the PDPA.
36 Section 26 of the PDPA.
37 Sections 11 and 12 of the PDPA.

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.[38] Where cookies used for behavioural targeting involve the collection and use of personal data, the individual's consent is required.[39] 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.[40] 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.

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.[41]

iv Specific regulatory areas

Minors

The PDPA does not contain special protection for minors (under 21 years of age).[42] 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

38 Sections 7.5–7.8, PDPA Selected Topics Guidelines.

39 Section 7.11, PDPA Selected Topics Guidelines.

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

41 Section 12.61, PDPA Key Concepts Guidelines.

42 Section 8.1, PDPA Selected Topics Guidelines.

guardians on the minor's behalf.[43] The Education Guidelines[44] 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),[45] 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.

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 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

43 Section 14(4) of the PDPA. See also discussion at Section 8.9 of the PDPA Selected Topics Guidelines.

44 Sections 2.5–2.8, PDPC Advisory Guidelines on the Education Sector, issued 11 September 2014.

45 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.

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 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 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:

a it has taken appropriate steps to ensure that it will comply with the data protection provisions while the personal data remains in its possession or control; and

46 Section 6 of the PDPC Healthcare Guidelines.

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

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.

b it has taken appropriate steps to ensure that 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.

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.[54]

The Key Concepts Guidelines[55] 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.

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.

Other examples given by the 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 Key Concepts Guidelines also set out the scope of contractual clauses at Section 19.5 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 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).

51 Regulation 9 of the PDP Regulations.

52 Regulation 10 of the PDP Regulations.

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

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

55 Issued on 23 September 2013 and revised on 8 May 2015.

S/N	Area of protection	Recipient	
		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

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.[56] Organisations must also develop a complaints mechanism,[57] and communicate to their staff the policies and practices they have implemented.[58] Information on policies and practices, including the complaints mechanism, is to be made available on request.[59] 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.[60]

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.

56 Section 12(a) of the PDPA.
57 Section 12(b) of the PDPA.
58 Section 12(c) of the PDPA.
59 Section 12(d) of the PDPA.
60 Section 11(4) of the PDPA.

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 this should be made available to the public.

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 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.[61] 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.[62] Further, an organisation may

61 Section 4(6) of the PDPA.

62 Second Schedule, Section 1(e) of the PDPA.

use personal data about an individual without the consent of the individual if the use is necessary for any investigation or proceedings.[63] 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.[64] 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 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.[65]

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,[66] carrying out investigations (whether on its on accord or upon a complaint), and prosecuting and adjudicating on certain matters arising out of the PDPA.[67]

To enable the PDPC to carry out its functions effectively, it has been entrusted with broad powers of investigation,[68] 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.[69] The PDPC may also in its discretion compound the offence.[70] Certain breaches can attract penalties of up to three years' imprisonment.[71] 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,

63 Third Schedule, Section 1(e) of the PDPA.

64 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.

65 Section 10(4) of the PDPA.

66 Section 28 of the PDPA.

67 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.

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

69 Section 29 of the PDPA.

70 Section 55 of the PDPA.

71 Section 56 of the PDPA.

or is attributable to his or her neglect.[72] 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.[73]

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.[74]

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.

ii Recent enforcement cases

In 2017, the PDPC published 19 decisions. In 2018, the number of published decisions stood at 17 by July 2018. 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 2017 and the first half of 2018 set out the PDPC's typical mix of behaviour remedies combined with financial penalties, including:

a *Jiwon Hair Salon*:[75] for the respondent's failure to fulfil the openness obligation under Section 12(a) of the PDPA, the PDPC directed the respondent to put in place a data protection policy to comply with the provisions of the PDPA.

b *Aviva Ltd* (October 2017):[76] PDPC issued a fine of S$6,000 to multinational insurance company Aviva Ltd because the organisation failed to make reasonable security arrangements around the mailing of follow-up letters to its policyholders, which allowed the accidental mailing of documents meant for one policyholder to another policyholder.

c *Aviva Ltd* (April 2018):[77] in a matter similar to the October 2017 *Aviva* action, PDPC issued a fine of S$30,000 for failing to make reasonable security arrangements to prevent the unauthorised disclosure of personal data of policyholders, which allowed the accidental mailing of underwriting letters meant for three different clients to another client. In reaching its penalty, the Commissioner noted that this incident was 'disappointingly similar' to the October 2017 matter.

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

72 Section 52 of the PDPA.

73 Section 53 of the PDPA.

74 Section 35 of the PDPA.

75 Decision Citation: [2018] SGPDPC 2.

76 Decision Citation: [2017] SGPDPC 14.

77 Decision Citation: [2018] SGPDPC 4.

organisation may be taken until after the right of appeal has been exhausted and the final decision is made.[78] 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.[79]

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 above, in the PDPC's public consultation of July through September 2017, the PDPC proposed incorporating a mandatory reporting requirement in certain circumstances. 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.

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.

ii Cybersecurity

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

In Singapore, the CMCA and the Cybersecurity Act are the key legislations governing cybercrime and cybersecurity. The CMCA is primarily focused on defining various cybercrime offences, including criminalising the unauthorised accessing[80] or modification of computer material,[81] use or interception of a computer service,[82] obstruction of use of a computer,[83]

78 Section 32 of the PDPA.

79 www.pdpc.gov.sg/docs/default-source/advisory-guidelines-on-enforcement/advisory-guidelines-on-enforcement-of-dp-provisions-(210416).pdf?sfvrsn=2.

80 Sections 3 and 4 of the CMCA.

81 Section 5 of the CMCA.

82 Section 6 of the CMCA.

83 Section 7 of the CMCA.

and unauthorised disclosure of access codes.[84] The 2017 amendments to the CMCA added the offences of obtaining or making available personal information that the offender believes was obtained through a computer crime[85] and using or supplying software or other items to commit or facilitate the commission of a computer crime.[86]

Although the CMCA is in general a criminal statute, the 2013 amendments added a cybersecurity provision in the event of certain critical cybersecurity threats. In particular, the Minister of Home Affairs may direct entities to take such pre-emptive measures as necessary to prevent, detect or counter any cybersecurity threat posed to national security, essential services or the defence of Singapore or foreign relations of Singapore.[87]

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.

X OUTLOOK

In keeping with its declared strategy, Singapore continues to progress on clarifying and enforcing its existing data privacy and cybersecurity regime.

84 Section 8 of the CMCA.

85 Section 8A of the CMCA.

86 Section 8B of the CMCA.

87 Section 15A of the CMCA. Essential services include the energy, finance and banking, ICT, security and emergency services, transportation, water, government and healthcare sectors.

Appendix 1

ABOUT THE AUTHORS

YUET MING THAM

Sidley Austin LLP

Yuet is a global head of the government litigation and investigations group, and head of the Asia Pacific compliance and investigations group. Besides compliance and investigations, Yuet focuses on privacy and cybersecurity work. She speaks fluent English, Mandarin, Cantonese and Malay and is admitted in New York, England and Wales, Hong Kong and Singapore.

Yuet was most recently awarded the emerging markets 'compliance and investigations lawyer of the year' by *The Asian/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' sector in *IFLR1000* as a 'leading lawyer' and has also been listed by *Who's Who Legal* as a 'leading business lawyer' in life sciences, business crime defence and investigations. In the 2018 edition of *Chambers Asia Pacific*, Yuet is described as 'exceptionally bright' and 'very responsive and knowledgeable and can immediately dive into the issues'. The 2015 edition of *Chambers Global* stated 'Ms. Tham is described by clients as 'a marvellous and gifted attorney'. 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

Level 31, Six Battery Road
Singapore 049909
Tel: +65 6230 3969
Fax: +65 6230 3939

yuetming.tham@sidley.com
www.sidley.com

ISBN 978-1-912228-62-1