The Privacy, Data Protection and Cybersecurity Law Review

Third Edition

Editor
Alan Charles Raul

Law Business Research

The Privacy, Data Protection and Cybersecurity Law Review

Third Edition

Editor
Alan Charles Raul

Law Business Research Ltd

PUBLISHER
Gideon Roberton

SENIOR BUSINESS DEVELOPMENT MANAGER
Nick Barette

BUSINESS DEVELOPMENT MANAGER
Thomas Lee

SENIOR ACCOUNT MANAGERS
Felicity Bown, Joel Woods

ACCOUNT MANAGERS
Jessica Parsons, Jesse Rae Farragher

MARKETING COORDINATOR
Rebecca Mogridge

EDITORIAL ASSISTANT
Gavin Jordan

HEAD OF PRODUCTION
Adam Myers

PRODUCTION EDITOR
Anne Borthwick

SUBEDITOR
Anna Andreoli

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 978-1-910813-32-4

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

THE LAW REVIEWS

THE MERGERS AND ACQUISITIONS REVIEW

THE RESTRUCTURING REVIEW

THE PRIVATE COMPETITION ENFORCEMENT REVIEW

THE DISPUTE RESOLUTION REVIEW

THE EMPLOYMENT LAW REVIEW

THE PUBLIC COMPETITION ENFORCEMENT REVIEW

THE BANKING REGULATION REVIEW

THE INTERNATIONAL ARBITRATION REVIEW

THE MERGER CONTROL REVIEW

THE TECHNOLOGY, MEDIA AND
TELECOMMUNICATIONS REVIEW

THE INWARD INVESTMENT AND
INTERNATIONAL TAXATION REVIEW

THE CORPORATE GOVERNANCE REVIEW

THE CORPORATE IMMIGRATION REVIEW

THE INTERNATIONAL INVESTIGATIONS REVIEW

THE PROJECTS AND CONSTRUCTION REVIEW

THE INTERNATIONAL CAPITAL MARKETS REVIEW

THE REAL ESTATE LAW REVIEW

THE PRIVATE EQUITY REVIEW

THE ENERGY REGULATION AND MARKETS REVIEW

THE INTELLECTUAL PROPERTY REVIEW

THE ASSET MANAGEMENT REVIEW

THE PRIVATE WEALTH AND PRIVATE CLIENT REVIEW

THE MINING LAW REVIEW

THE EXECUTIVE REMUNERATION REVIEW

THE ANTI-BRIBERY AND ANTI-CORRUPTION REVIEW

THE CARTELS AND LENIENCY REVIEW

THE TAX DISPUTES AND LITIGATION REVIEW

THE LIFE SCIENCES LAW REVIEW

THE INSURANCE AND REINSURANCE LAW REVIEW

THE GOVERNMENT PROCUREMENT REVIEW

THE DOMINANCE AND MONOPOLIES REVIEW

THE AVIATION LAW REVIEW

THE FOREIGN INVESTMENT REGULATION REVIEW

THE ASSET TRACING AND RECOVERY REVIEW

THE INSOLVENCY REVIEW

THE OIL AND GAS LAW REVIEW

THE FRANCHISE LAW REVIEW

THE PRODUCT REGULATION AND LIABILITY REVIEW

THE SHIPPING LAW REVIEW

THE ACQUISITION AND LEVERAGED FINANCE REVIEW

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

THE PUBLIC-PRIVATE PARTNERSHIP LAW REVIEW

THE TRANSPORT FINANCE LAW REVIEW

THE SECURITIES LITIGATION REVIEW

THE LENDING AND SECURED FINANCE REVIEW

THE INTERNATIONAL TRADE LAW REVIEW

THE SPORTS LAW REVIEW

THE INVESTMENT TREATY ARBITRATION REVIEW

THE GAMBLING LAW REVIEW

THE INTELLECTUAL PROPERTY AND ANTITRUST REVIEW

THE REAL ESTATE, M&A AND PRIVATE EQUITY REVIEW

THE SHAREHOLDER RIGHTS AND ACTIVISM REVIEW

www.TheLawReviews.co.uk

ACKNOWLEDGEMENTS

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

ALLENS

ASTREA

BAKER & MCKENZIE - CIS, LIMITED

BOGSCH & PARTNERS LAW FIRM

CMS CAMERON MCKENNA GRESZTA I SAWICKI SP.K

DUNAUD CLARENC COMBLES & ASSOCIÉS

ELIG, ATTORNEYS-AT-LAW

GIANNI, ORIGONI, GRIPPO, CAPPELLI & PARTNERS

JUN HE LAW OFFICES

LEE & KO

MATHESON

NNOVATION LLP

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SIQUEIRA CASTRO – ADVOGADOS

SK CHAMBERS

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

VIEIRA DE ALMEIDA & ASSOCIADOS, SP RL

WALDER WYSS LTD

WINHELLER RECHTSANWALTSGESELLSCHAFT MBH

CONTENTS

Chapter 23

SINGAPORE

Yuet Ming Tham[1]

I OVERVIEW

The Personal Data Protection Act 2012 (PDPA) is Singapore's first comprehensive framework established to ensure the protection of personal data. The Bill was passed in 2012, but implementation was in phases so that organisations had 18 months to bring their activities into compliance with the PDPA. Provisions relating to the Do Not Call (DNC) Registry came into force on 2 January 2014 whereas the substantive data protection provisions subsequently came into force on 2 July 2014. Under the Act, the Personal Data Protection Commission (PDPC) was set up to administer and enforce the Act.

Before the PDPA, data protection obligations were sector-specific and limited in scope. With a growing list of countries enacting similar laws, there was a strong need to bring Singapore's data protection regime on par with international standards and facilitate cross-border transfers of data. Indeed, Singapore sees the PDPA as an essential regime to 'enhance its competitiveness and strengthen our position as a trusted business hub',[2] necessary to achieving Singapore's aspirations of being a choice location for data hosting and management activities.

One notable feature of the PDPA is that government agencies do not fall within the ambit of the PDPA. The reason for this, as discussed in parliament, is that government agencies collect data where necessary to carry out their regulatory and statutory functions. In any event, the public sector is governed by similar data protection rules, some of which are even stricter that the PDPA.[3]

In this chapter, we will outline the key aspects of the PDPA, which includes a brief discussion of the key concepts, the obligations imposed on data handlers, and the interplay

1 Yuet Ming Tham is a partner at Sidley Austin.

2 Yaacob Ibrahim, Minister for Information, Communications and the Arts, in the Second Reading Speech on the Personal Data Protection Bill 2012.

3 Ibid.

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. In relation to cybersecurity, Singapore has recently beefed up its laws in this regard and recognised the potentially devastating effects in the event of a compromise or data breach. Finally, we will highlight future developments to keep a close eye on.

II THE YEAR IN REVIEW

There have been a few clarifications and updates to the PDPA and to its subsidiary legislation. A selection of the most significant of these is set out below.

On 9 June and 15 July 2016, the Advisory Guidelines on Key Concepts in the Personal Data Protection Act (Key Concepts Guidelines) were revised. Chapter 12 of the Key Concepts Guidelines has been revised to provide further clarity on the withdrawal of consent requirements, including how organisations are to facilitate and effect withdrawal of consent requests (updated 15 July 2016). Chapter 15 of the Key Concepts Guidelines has also been revised to provide further clarify how organisations should handle access requests in certain situations, and the preservation of the requested personal data by organisations when processing or after rejecting an access request (updated 9 June 2016). Further, the section that was previously labelled under the Do Not Call provision in the Key Concepts Guidelines has been incorporated into the Advisory Guidelines on the Do Not Call Provisions as of 15 July 2016.

On 9 June 2016, the Advisory Guidelines on the Personal Data Protection Act for Selected Topics was updated to give further clarity regarding an organisation's obligation to provide access to personal data in CCTV footage. The PDPC provided further guidance on CCTV footage concerning:

a the content of notices when CCTV is deployed;
b the obligations of organisations regarding access requests to CCTV footage;
c the reasons available that are sufficient for organisations to deny access to CCTV footage;
d the withdrawal of consent by individuals;
e the format in which organisations are able to provide individuals with a copy of CCTV footage; and
f disclaimers regarding the efficacy of 'video masking'.

On 21 April 2016, the PDPC published a set of new Advisory Guidelines on the Enforcement of the Data Protection Provisions (Enforcement Guidelines). Under the PDPA, organisations are subject to certain obligations for personal data protection (Data Protection Provisions), including the obligation to implement reasonable security for the personal data. The Enforcement Guidelines provide guidance on the manner in which the PDPC will interpret the Data Protection Provisions, and they are advisory in nature and are not legally binding on the PDPC or any other party. The Enforcement Guidelines provide guidance on the PDPC's preferred approached when handling complaints relating to a breach of the Data Protection Provisions, possible factors leading to an investigation and considerations affecting the calculation of a penalty. The Enforcement Guidelines also provide guidance for organisations

intending to issue any media releases or public disclosure of matters related to the alleged breach. Such organisations are advised to consider whether such release or disclosure would hinder the ongoing investigation, and also to provide the PDPC with a copy of the materials before their release.

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.[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 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.[11]

4 Section 2 of the PDPA.

5 Section 5.28, PDPC Advisory Guidelines on Key Concepts in the Personal Data Protection Act, issued on 24 September 2013 and revised on 8 May 2015 (PDPA Key Concepts Guidelines).

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.

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 its 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 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]

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.[20]

As mentioned in Section I, *supra*, to ease organisations into the new data protection regime, 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, such consent may be presumed. Consent may be

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

13 Section 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.

20 Section 6 of the PDPA.

21 Section 13 to 17 of the PDPA.

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 part 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.

Notification[25]

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

---

22 In Paragraph 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 Paragraph 12.32, PDPA Key Concepts Guidelines.

24 Section 18 of the PDPA.

25 Section 20 of the PDPA.

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

27 Sections 21 and 22 of the PDPA.

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

29 Paragraph 15.34, PDPA Key Concepts Guidelines.

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 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[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 such personal data.[32]

Retention limitation[33]
An organisation may not retain such 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[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, *infra*).

Openness[35]
An organisation is obliged to implement necessary policies and procedures in compliance with the PDPA, and to ensure that such information is available publicly.

iii Technological innovation and privacy law

The PDPC considers that an IP address or network identifier, such as an IMEI 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 such information

30 Section 23 of the PDPA.

31 Section 24 of the PDPA.

32 See discussion in Paragraphs 17.1–17.3, PDPC Key Concepts Guidelines.

33 Section 25 of the PDPA.

34 Section 26 of the PDPA.

35 Sections 11 and 12 of the PDPA.

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.

As regards social media, one issue arises where personal data are disclosed on social networking platforms and becomes 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

36 Section 7.5–7.8, PDPC Advisory Guidelines on the Personal Data Protection Act for Selected Topics, issued 24 September 2013 and revised 11 September 2014 (PDPA Selected Topics Guidelines).

37 Ibid., Paragraph 7.11.

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

39 Paragraph 12.55, PDPA Key Concepts Guidelines.

40 Section 8.1, PDPA Selected Topics Guidelines.

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] provide that various financial institutions are required to:

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.

MAS will have 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.

41 Section 14(4) of the PDPA. See also discussion at Section 8.8 of the PDPA Selected Topics Guidelines.

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

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-changer's 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.

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 Healthcare Guidelines[44] 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.[45] 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.[46] Other legal obligations, such as to protect confidential information of their employees, will nevertheless continue to apply.[47]

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

---

44 Section 6 of the PDPC Advisory Guidelines for the Healthcare Sector, issued 11 September 2014.

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

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

47 Sections 5.13 to 5.17 of the PDPA Selected Topics Guidelines.

IV 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.[48]

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

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.[49] 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.[50]

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;[51] 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.[52]

The Key Concepts Guidelines [53] 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.

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

49 Regulation 9 of the PDP Regulations.

50 Regulation 10 of the PDP Regulations.

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

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

53 Issued on 23 September 2013, and revised on 8 May 2015.

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).

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

V COMPANY POLICIES AND PRACTICES

Organisations are obliged to develop and implement policies and practices necessary to meet their obligations under the PDPA.[54] Organisations must also develop a complaints mechanism,[55] and communicate to their staff the policies and practices they have implemented.[56] Information on policies and practices, including the complaints mechanism, is to be made available on request.[57] 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.[58]

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

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

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 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 e-mails, 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 DISCOVERY AND DISCLOSURE

The data protection provisions under the PDPA do not affect any rights or obligations under other laws.[59] As such, where the law mandates disclosure of information that may include personal data, another law would prevail to the extent 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 such collection is necessary for any investigation or proceedings, so as not to compromise the availability or accuracy of the personal data.[60] Further, an organisation may use personal data about an individual without the consent of the individual if such use is necessary for any investigation or proceedings.[61] 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.[62] 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.[63]

VII 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,[64] carrying out investigations (whether on its on accord or upon a complaint), and prosecuting and adjudicating on certain matters arising out of the PDPA.[65]

To enable the PDPC to carry out its functions effectively, it has been entrusted with broad powers of investigation,[66] including the power to require organisations to produce

59 Section 4(6) of the PDPA.

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

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

62 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.

63 Section 10(4) of the PDPA.

64 Section 28 of the PDPA.

65 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.

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

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.[67] The PDPC may also in its discretion compound the offence.[68] Certain breaches can attract penalties of up to three years' imprisonment.[69] 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.[70] 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.[71]

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.[72]

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

On 21 April 2016, the PDPC took enforcement actions against several organisations for breaching their data protection obligations under the PDPA. Such enforcement actions include:

a A financial penalty of S$50,000 imposed on K Box Entertainment Group Pte Ltd (K Box), a karaoke chain, for not putting in place sufficient security measures to protect the personal data of 317,000 members, for inadequate data protection policies and the absence of a data protection officer. Further, the PDPC imposed a financial penalty of S$10,000 on Finantech Holdings Pte Ltd, the IT vendor in charge of K Box's content management system (as K Box's data intermediary).

b For failing to put in place adequate security measures to protect personal data in its possession that affected 4,000 members, the PDPC imposed a financial penalty of S$10,000 on the Institution of Engineers, Singapore. For a similar breach that affected more than 900 customers, a financial penalty of S$5,000 was imposed on Fei Fah Medical Manufacturing Pte Ltd, a health supplements supplier.

c For unauthorised disclosure of 37 customers' personal data to four individuals, the PDPC issued directions to Universal Travel Corporation Pte Ltd, a tour agency, to enhance its personal data policies.

67 Section 29 of the PDPA.

68 Section 55 of the PDPA.

69 Section 56 of the PDPA.

70 Section 52 of the PDPA.

71 Section 53 of the PDPA.

72 Section 35 of the PDPA.

d The PDPC also issued warnings to six organisations for lapses in handling personal data:
- Challenger Technologies Ltd, an IT retailer, as well as its IT vendor, Xirlynx Innovations;
- Full House Communications Pte Ltd, a consumer home show organiser;
- Metro Pte Ltd, a retailer;
- Singapore Computer Society, an infocomm and digital media professional society; and
- YesTuition Agency, a tuition agency.

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 until after the right of appeal has been exhausted and the final decision is made.[73] 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. [74]

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, there is no requirement to notify authorities in the event of a data breach. There are, however, industry-specific guidelines and notices that have imposed such reporting obligations. In that regard, MAS issued a set of notices to financial institutions on 1 July 2014 to direct that all security breaches should be reported to the MAS within one hour of discovery.

ii Cybersecurity

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

73 Section 32 of the PDPA.

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

In Singapore, the Computer Misuse and Cybersecurity Act (Cybersecurity Act) is the key legislation governing cybercrime and cybersecurity. In particular, it regulates unauthorised access to or modification of computer material;[75] unauthorised use or interception of a computer service;[76] and unauthorised disclosure of access codes.[77]

The Cybersecurity Act was amended in 2013 to address cyberthreats to critical information infrastructure, namely systems necessary for the delivery of essential services to the public in key sectors.[78] 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 the national security, essential services or defence of Singapore or foreign relations of Singapore.[79]

Additionally, Singapore's Minister for Communications and Information, Dr Yaacob Ibrahim, announced that the government would develop a Cybersecurity Act in 2017. The Minister outlined four prospective features:

a assurance that critical information infrastructure (e.g., energy, water, transportation, government, media, security and emergency services) operators are proactive in maintaining cybersecurity;

b a mandatory reporting requirement for security breaches;

c wider powers for the Cyber Security Agency to manage cybersecurity incidents; and

d higher standards for cybersecurity providers.

X OUTLOOK

With the issuance of more guidelines, we expect to see a higher level of compliance and control in Singapore's data privacy and cybersecurity scene. The conscious effort made by the government to address the need to help organisations enhance IT security, especially small and medium-sized enterprises, is also something that is apparent from the new developments. It is also likely that Singapore will see more industry-led guidelines.

It is anticipated that the government will continue to place more emphasis on developing Singapore's cybersecurity framework and focus on the protection of networks from cybersecurity attacks.

Finally, we can expect further collaboration between the government, the private sector and trade associations to promote and strengthen Singapore's cybersecurity and data protection regime.

75 Sections 3 and 5 of the Computer Misuse and Cybersecurity Act 2013.

76 Section 6 of the Computer Misuse and Cybersecurity Act 2013.

77 Section 8 of the Computer Misuse and Cybersecurity Act 2013.

78 This would include the energy, finance and banking, ICT, security and emergency services, transportation, water, government and healthcare sectors.

79 Section 15A of the Computer Misuse and Cybersecurity Act 2013.

Appendix 1

ABOUT THE AUTHORS

YUET MING THAM

Sidley Austin

Yuet Ming Tham is a partner in Sidley Austin's Hong Kong and Singapore offices. She advises international corporations on their legal risks, such as those relating to privacy, data protection and cybersecurity law issues, as well as cross-border compliance and investigations, anti-bribery laws (including FCPA), international trade controls, sanctions, anti-money laundering and dispute resolution.

Prior to joining Sidley, Yuet was the Asia head of the regulatory, compliance and investigations group, and also head of the Asia life sciences group at another international law firm. She has also held roles as a deputy public prosecutor in Singapore and was the Asia Pacific regional compliance director for Pfizer. During that time, she was responsible for compliance and investigations in Singapore, Japan, China, Australia, Korea, India, Indonesia, Thailand, Taiwan, Hong Kong, Malaysia and the Philippines.

Yuet is named as a leading lawyer in *Chambers Asia Pacific* in four categories, as well as being recognised in *IFLR1000* and *The Legal 500 – Asia Pacific*. In 2014, she was the only lawyer awarded the Client Choice award by International Law Office for white-collar crime practice in Hong Kong. The leading legal directory, *Chambers Asia Pacific*, noted that industry players appreciate Yuet's 'wealth of knowledge of the latest trends across the region', as well as her having a 'tough, no-nonsense approach in tackling tricky compliance questions'. In the global edition of the book, she is described by clients as 'a marvelous and gifted attorney', and a client observed that 'two things stand out about her: she is extraordinarily responsive, but is also very good at getting answers to your questions from a practical perspective. In that respect, she really is a gem of a lawyer'. Yuet has up-to-the-minute knowledge on the rapidly changing issues surrounding privacy, data protection and cybersecurity matters related to Hong Kong, Singapore and the rest of Asia. She has written several articles and is a frequent speaker at industry conferences on these subjects.

She speaks English, Mandarin, Cantonese and Malay, and is admitted to practise in Hong Kong, Singapore, New York, and England and Wales.

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

Level 31, Six Battery Road
Singapore 049909
Tel: +65 6230 3969
Fax: +65 6230 3939
yuetming.tham@sidley.com