THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

NINTH EDITION

Editor
Alan Charles Raul

THE LAWREVIEWS

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

NINTH EDITION

Reproduced with permission from Law Business Research Ltd
This article was first published in October 2022
For further information please contact Nick.Barette@thelawreviews.co.uk

Editor
Alan Charles Raul

THE LAWREVIEWS

PUBLISHER
Clare Bolton

HEAD OF BUSINESS DEVELOPMENT
Nick Barette

TEAM LEADER
Katie Hodgetts

SENIOR BUSINESS DEVELOPMENT MANAGER
Rebecca Mogridge

BUSINESS DEVELOPMENT MANAGERS
Joey Kwok

BUSINESS DEVELOPMENT ASSOCIATE
Archie McEwan

RESEARCH LEAD
Kieran Hansen

EDITORIAL COORDINATOR
Leke Williams

PRODUCTION AND OPERATIONS DIRECTOR
Adam Myers

PRODUCTION EDITOR
Louise Robb

SUBEDITOR
Martin Roach

CHIEF EXECUTIVE OFFICER
Nick Brailey

Published in the United Kingdom
by Law Business Research Ltd, London
Holborn Gate, 330 High Holborn, London, WC1V 7QT, UK

www.TheLawReviews.co.uk

ISBN 978-1-80449-116-4

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

ACKNOWLEDGEMENTS

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

ANDERSON LLOYD

ANJIE LAW FIRM

ASTREA

AZEVEDO SETTE ADVOGADOS

BOGSCH & PARTNERS LAW FIRM

BOMCHIL

CHRISTOPHER & LEE ONG

CLEMENS

CTSU, SOCIEDADE DE ADVOGADOS, SP, RL, SA

GREENBERG TRAURIG LLP

KALUS KENNY INTELEX

KHODEIR AND PARTNERS

K&K ADVOCATES

KPMG CHINA

LECOCQASSOCIATE

LEE, TSAI & PARTNERS

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

WALDER WYSS LTD

WINHELLER ATTORNEYS AT LAW & TAX ADVISORS

CONTENTS

Chapter 24

SINGAPORE

Margaret Hope Allen, Yuet Ming Tham and Faraaz Amzar[1]

I OVERVIEW

In 2021 and 2022, Singapore continued to develop its data protection, cybercrime and cybersecurity regimes. As set out in Singapore's Cyber Landscape 2019 report,[2] the government has focused on four pillars of strategy to protect the country from cyberthreats and reinforce Singapore's standing as a leading information systems hub. It is aimed at building a resilient infrastructure, creating a safer cyberspace environment, developing a vibrant cybersecurity ecosystem and strengthening international partnerships. The key legal components in this strategy include the Personal Data Protection Act 2012 (PDPA), Singapore's first comprehensive framework established to ensure the protection of personal data, the accompanying Personal Data Protection Regulations 2014, the Computer Misuse Act (CMA) to combat cybercrime and other cyberthreats, and the Cybersecurity Act 2018 (Cybersecurity Act), which focuses on protecting Singapore's Critical Information Infrastructure (CII) in 11 critical sectors and establishing a comprehensive national cybersecurity framework. In November 2020, Singapore's legislature approved amendments to the PDPA. Amendments to the PDPA are being implemented in phases, with some amendments having taken effect on 1 February 2021 and 1 October 2021.

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

1 Margaret Hope Allen and Yuet Ming Tham are partners and Faraaz Amzar is an associate at Sidley Austin LLP.

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

II THE YEAR IN REVIEW

i PDPA developments

There were a number of significant developments related to the PDPA and the Personal Data Protection Commission (PDPC – the body set up to administer and enforce the PDPA) from July 2021 to June 2022.

In November 2020, Singapore's legislature approved important amendments to the PDPA, which took effect in phases, beginning on 1 February 2021. Important changes have been introduced to the PDPA, including the introduction of a mandatory data notification requirement and a new legitimate interests exception. These changes are discussed in detail below.

Significantly, from 1 October 2022, the maximum financial penalties for data breaches by organisations will be raised to S$1 million or 10 per cent of local annual turnover for organisations whose turnover exceeds S$10 million, whichever is higher. The penalties imposed under the PDPA could therefore be more stringent than under the European Union's General Data Protection Regulation, which presently imposes fines of up to €20 million or 4 per cent worldwide turnover, whichever is higher.

The PDPC increasingly emphasises the principle of accountability in the context of personal data protection and has provided guidance on how organisations may demonstrate accountability for personal data in their care. The PDPC has also published new guidance and revised existing guidelines to help organisations comply with the new requirements under the amended PDPA, including the Guide on Managing and Notifying Data Breaches (Data Breach Notification Guide) under the PDPA,[3] the Advisory Guidelines on Key Concepts in the Personal Data Protection Act[4] and the Advisory Guidelines on the Personal Data Protection Act for Selected Topics.[5]

ii CMA developments and the Cybersecurity Act

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

The CMA was amended in 2013 and again in 2017 to strengthen the country's response to national level cyberthreats. The amendments broadened the scope of the CMA by criminalising certain conduct not already covered by the existing law and enhancing penalties in certain situations (for example, the amended CMA criminalises the use of stolen data to carry out a crime even if the offender did not steal the data himself or herself, and prohibits the use of programs or devices used to facilitate computer crimes, such as malware or code crackers). The amendments also extended the extraterritorial reach of the CMA by covering actions by persons targeting systems that result in, or create a significant risk of, serious harm in Singapore, even if the persons and systems are both located outside Singapore.

3 https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-on-Managing-and-Notifying-Data-Breaches-under-the-PDPA-15-Mar-2021.pdf?la=en.

4 https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Advisory-Guidelines-on-Key-Concepts-in-the-PDPA-17-May-2022.ashx?la=en.

5 https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Selected-Topics/Advisory-Guidelines-on-the-PDPA-for-Selected-Topics-17-May-2022.ashx?la=en.

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

In recent years, the Singapore government has observed that since the Cybersecurity Act was first introduced in 2018, there has been significantly greater reliance on digital infrastructure and services. With increasing digitalisation, more organisations are at risk of falling victim to cyber-attacks if cybersecurity safeguards are not updated and modernised. The Ministry of Communications and Information has therefore announced a review of the Cybersecurity Act and its accompanying Code of Practice, expected to begin in 2023.

iii Recent developments and regulatory compliance

Although the developments with the CMA and the Cybersecurity Act represent significant milestones in Singapore's overall cybersecurity strategy, the key compliance framework from the perspective of companies and organisations remains at this point with data protection and privacy. The CMA is primarily a criminal statute, and the government has not issued any regulations or guidelines for the CMA. The Cybersecurity Act imposes a number of legal requirements on CII owners and cybersecurity service providers, but until the government issues implementing regulations or advisory guidance regarding these new requirements, organisations' focus will be on the PDPA and its related regulations, subsidiary legislation and advisory guidelines.[6] In November 2021, Singapore experienced its most serious data privacy breach when the hospitality platform RedDoorz was found to have compromised the security of 5.9 million customer records in the largest data breach incident since the PDPA came into force. The PDPC fined local firm Commeasure, which operates the RedDoorz website, S$74,000. This is significantly lower than the combined S$1 million fine imposed on SingHealth and Integrated Health Information Systems for the 2018 breach that affected 1.5 million people. Interestingly, one of the mitigatory factors that the PDPC considered in deciding the amount of financial penalty to be imposed on Commeasure was the hardship faced by the hospitality sector as a result of the covid-19 pandemic.

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. Consent can be expressed or deemed under certain circumstances.

There is no prescribed list of personal data; rather, these are defined broadly as data about an individual, whether or not it is 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.[7]

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

7 Section 2 of the PDPA.

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 is sensitive, or between data that is in electronic or hard copy formats. There are also no ownership rights conferred on personal data to individuals or organisations.[8] There are certain exceptions to which the PDPA would apply. Business contact information of an individual generally falls outside the ambit of the PDPA,[9] as does personal data that is publicly available.[10] In addition, personal data of an individual who has been deceased for over 10 years[11] and personal data contained within records for over 100 years is exempt.[12]

Pursuant to the PDPA, organisations are responsible for personal data in their possession or under their control.[13] Organisations include individuals in Singapore, whether or not they are residents, local and foreign companies, associations and bodies (incorporated and unincorporated), whether or not they have an office or a place of business in Singapore.[14] The PDPA does not apply to public agencies.[15] 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.[16]

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, retention and data breach notification obligations under the PDPA. The organisation that engaged a data intermediary's services remains fully responsible in respect of the data as if it had processed the data on its own.[17]

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.[18]

Subsidiary legislation to the PDPA includes implementing regulations relating to the Do Not Call (DNC) Registry,[19] enforcement,[20] composition of offences,[21] requests for access to and correction of personal data, the transfer of personal data outside Singapore[22] and notification of data breaches.[23]

There is also sector-specific legislation, such as the Banking Act, the Telecommunications Act and the Private Hospitals and Medical Clinics Act, imposing specific data protection

8 Sections 5.27 to 5.29, Advisory Guidelines on Key Concepts in the PDPA (PDPA Key Concepts Guidelines) issued on 23 September 2013 and revised on 1 February 2021.

9 Section 4(5) of the PDPA.

10 First Schedule, Part 2, Paragraph 1 of the PDPA.

11 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.

12 Section 4(4) of the PDPA.

13 Section 11(2) of the PDPA.

14 Section 2 of the PDPA.

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

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

17 Section 4(3) of the PDPA.

18 Section 48O of the PDPA.

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

20 Personal Data Protection (Enforcement) Regulations 2021.

21 Personal Data Protection (Composition of Offences) Regulations 2021.

22 Personal Data Protection Regulations 2021.

23 Personal Data Protection (Notification of Data Breaches) Regulations 2021.

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.[24]

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 10 key obligations in relation to how organisations collect, use and disclose personal data, as briefly described below.

Consent

An organisation may only collect, use or disclose personal data for purposes to which an individual has consented.[25] Where the individual has provided the information voluntarily and it was reasonable in the circumstances, the consent may be deemed. Further, consent may also be deemed by notification. An individual is deemed to have consented to the collection, use or disclosure of personal data for a purpose that he or she has been notified of, and he or she has not notified the organisation that he or she does not consent to such collection, use or disclosure within a reasonable period.[26] The PDPA does not specify what is a reasonable period. To rely on this basis to deem consent, an organisation must first conduct an assessment to determine that the proposed collection, use or disclosure of personal data is not likely to have an adverse effect on the individual. Consent may also be deemed by contractual necessity.[27] Consent (whether express or deemed) may be withdrawn at any time with reasonable notice.[28] 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.

The First Schedule and Second Schedule of the PDPA sets out exceptions where an organisation may collect, use or disclose personal data without the consent of the individual. When the PDPA was amended in 2021, a new exception on the basis of legitimate interest was introduced to the PDPA.[29] If the collection, use or disclosure of personal data is in the legitimate interests of the organisation or another person, and such legitimate interests outweigh any adverse effect on the individual, the organisation may rely on the exception. Legitimate interests generally refer to any lawful interests of an organisation or other person.[30]

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

25 Sections 13 to 17 of the PDPA.

26 Section 15A of the PDPA.

27 Section 15(3) of the PDPA.

28 In Section 12.41 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.

29 Part 3 of First Schedule of the PDPA.

30 Section 12.45 of the PDPA Key Concepts Guidelines.

Paragraphs 2 to 10 of Part 3 of the First Schedule of the PDPA set out specific purposes that would generally be considered legitimate interests, including evaluative purposes, investigations or proceedings and recovery of debt. Purposes that do not fall under the aforementioned specific purposes may still be considered legitimate interests, but if a purpose does not fall within Paragraphs 2 to 10 of Part 3 of the First Schedule of the PDPA, an organisation must first conduct an assessment to assess the adverse effect and ensure that the legitimate interests outweigh any adverse effect.

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 for the collection, use and disclosure of an individual's personal data for the purposes of the other organisations within the corporate group.[31]

Purpose limitation

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.[32]

Notification

Organisations are obliged to notify individuals of their purposes for the collection, use and disclosure of the personal data on or before the collection.[33] 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.[34]

Access and correction

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 explain how the said personal data has been or may have been used or disclosed by the organisation during the past year.[35] 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.[36]

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.[37]

31 Section 12.31, PDPA Key Concepts Guidelines.

32 Section 18 of the PDPA.

33 Section 20 of the PDPA.

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

35 Sections 21 and 22 of the PDPA.

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

37 Section 15.18, PDPA Key Concepts Guidelines.

Accuracy

An organisation is obliged to make a reasonable effort to ensure that the personal data collected by or on behalf of the organisation is accurate and complete if it is likely to be used to make a decision that affects an individual or is likely to be disclosed to another organisation.[38]

Protection

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.[39] 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.[40]

Retention limitation

An organisation may not retain personal data for longer than is reasonable for the purpose for which it was collected, and for no longer than is necessary in respect of its business or legal purposes.[41] Beyond that retention period, organisations should either delete or anonymise their records.

Transfer limitation

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[42] (see Section IV).

Accountability

Previously known as the openness obligation, under the accountability obligation, an organisation is held to be responsible for personal data in its possession or under its control.[43] To that end, it is obliged to designate one or more individuals to be responsible for ensuring the organisation's compliance with the PDPA, implementing necessary policies and procedures in compliance with the PDPA, and ensuring that this information is available on request.

Data breach notification

Once an organisation has reason to believe a data breach has occurred, it is required to conduct an assessment to determine whether the data breach is notifiable in a reasonable and expeditious manner.[44] Data intermediaries are also required to notify the organisation or public agency for which they process personal data if a data breach is detected. A data breach is notifiable if it results in, or is likely to result in, significant harm to an affected individual, or if it is, or is likely to be, of a significant scale. A data breach is deemed to result

38 Section 23 of the PDPA.
39 Section 24 of the PDPA.
40 See discussion in Sections 17.1–17.3, PDPA Key Concepts Guidelines.
41 Section 25 of the PDPA.
42 Section 26 of the PDPA.
43 Sections 11 and 12 of the PDPA.
44 Sections 26A to 26E of the PDPA.

in significant harm to an individual if the data breach relates to certain types of personal data, such as an individual's full name or identification number.[45] A data breach is deemed to be of a significant scale if the number of affected individuals is not fewer than 500. To demonstrate that is has taken reasonable and expeditious steps to assess whether a data breach is notifiable, the organisation must document all steps taken in the assessment.[46] A notifiable data breach must be notified to the PDPC as soon as is practicable, but in any case no later than three calendar days after the day of assessment. In addition, if the breach is notifiable on the ground that it results in, or is likely to result in, significant harm to an affected individual, the organisation must also notify each affected individual in any manner that is reasonable in the circumstances at the same time or after it notifies the PDPC. However, an organisation need not notify the affected individuals if it has taken remedial actions that render the data breach unlikely to result in significant harm to the affected individuals, or if appropriate technological measures were applied to the personal data before the data breach, rendering the personal data inaccessible or unintelligible to an unauthorised party.

iii Technological innovation and privacy law

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

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

Depending on the purpose for the use of cookies, the PDPA would apply only where cookies collect, use or disclose personal data. Thus, in respect of session cookies that only collect and store technical data, consent is not required.[47] Where cookies used for behavioural targeting involve the collection and use of personal data, the individual's consent is required.[48] 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.[49] 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

45 Section 3(1) of the Personal Data Protection (Notification of Data Breaches) Regulations 2021.

46 Page 22 of Data Breach Notification Guide.

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

48 Section 6.11, PDPA Selected Topics Guidelines.

49 Section 10 of the Personal Data Protection Regulations 2021.

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 was publicly available at the point of collection, the organisation will be able to use and disclose the same without consent.[50]

iv Specific regulatory areas

Minors

The PDPA does not contain special protection for minors (under 21 years of age).[51] However, the Selected Topics Advisory Guidelines note that a minor of 13 years or older typically has sufficient understanding to provide consent on his or her own behalf. Where a minor is below the age of 13, an organisation should obtain consent from the minor's parents or legal guardians on the minor's behalf.[52] The Education Guidelines[53] 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),[54] 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

50 Section 12.61, PDPA Key Concepts Guidelines.

51 Section 7.1, PDPA Selected Topics Guidelines.

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

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

54 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.

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.

On 5 December 2019, the MAS issued two further notices: a Notice on Cyber Hygiene[55] to licensees and operators of designated payment systems, and a Notice on Technology Risk Management[56] to operators and settlement institutions of designated payment systems, pursuant to Section 102(1) of the Payment Services Act 2019. They set out, among other things, cybersecurity requirements to protect customer information from unauthorised access or disclosure.

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

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

Electronic marketing

The PDPA contains provisions regarding the establishment of a national DNC Registry and obligations for organisations that send certain kinds of marketing messages to Singapore telephone numbers to comply with these provisions. The PDPA Healthcare Guidelines[57] 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 an 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 its collection, use and

55 MAS Notice PSN06.

56 MAS Notice PSN05.

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

disclosure.[58] 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, its collection, use or disclosure.[59] Other legal obligations, such as to protect confidential information of employees, will nevertheless continue to apply.[60]

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

IV INTERNATIONAL DATA TRANSFER AND DATA LOCALISATION

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.[61]

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

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

b the recipient is bound by legally enforceable obligations to protect the personal data in accordance with standards comparable to the PDPA.[62]

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.[63]

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;[64] or where the transfer is necessary for the performance of a contract. Alternatively, if an overseas recipient is Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules certified or APEC Privacy Recognition for Processors certified (where the recipient is a data intermediary), the recipient will be taken to be bound by legally enforceable obligations to provide a standard of protection that is at least comparable to the PDPA.[65]

58 Paragraph 10(b), Part 3 of First Schedule of the PDPA.

59 Paragraph 2, Part 3 of First Schedule of the PDPA.

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

61 Section 26(1) of the PDPA. The conditions for the transfer of personal data overseas are specified within the Personal Data Protection Regulations 2021 (PDP Regulations).

62 Regulation 10 of the PDP Regulations.

63 Regulation 11 of the PDP Regulations.

64 Regulation 10 of the PDP Regulations.

65 Regulation 12 of the PDP Regulations.

In respect of personal data that simply passes through servers in Singapore en route to an overseas destination, the transferring organisation will be deemed to have complied with the transfer limitation obligation.[66]

The PDPA Key Concepts Guidelines also provide examples to illustrate situations in which organisations are deemed to have transferred personal data overseas in compliance with their transfer limitation obligation pursuant to Section 26 of the PDPA, regardless of whether the foreign jurisdiction's privacy laws are comparable to the PDPA. An example is when a tour agency needs to share a customer's details (e.g., his or her name and passport number) to make hotel and flight bookings. The tour agency is deemed to have complied with Section 26 as the transfer is necessary for the performance of the contract between the agency and the customer.[67]

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

The PDPA Key Concepts Guidelines also sets out the scope of contractual clauses at Section 19.9 for recipients to comply with the required standard of protection in relation to personal data received so that it is comparable to the protection under the PDPA. The PDPA Key Concepts Guidelines sets out in a table (reproduced below) the areas of protection a transferring organisation should minimally set out in its contract in two situations: where the recipient is another organisation (except a data intermediary); and where the recipient is a data intermediary (i.e., an organisation that processes the personal data on behalf of the transferring organisation pursuant to a contract).

No.	Area of protection	Recipient is:	
		Data intermediary	Organisation (except data intermediary)
1	Purpose of collection, use and disclosure by recipient	–	Yes
2	Accuracy	–	Yes
3	Protection	Yes	Yes
4	Retention limitation	Yes	Yes
5	Policies on personal data protection	–	Yes
6	Access	–	Yes
7	Correction	–	Yes
8	Data breach notification	Yes, to notify organisation of data breaches without undue delay	Yes, to assess and notify the Commission/affected individuals of data breaches, where relevant

V COMPANY POLICIES AND PRACTICES

Organisations are obliged to develop and implement policies and practices necessary to meet their obligations under the PDPA.[68] Organisations must also develop a complaints mechanism,[69] and communicate to their staff the policies and practices they have

66 Regulation 10 of the PDP Regulations.

67 Section 19.8 of the PDPA Key Concepts Guidelines.

68 Section 12(a) of the PDPA.

69 Section 12(b) of the PDPA.

implemented.[70] Information on policies and practices, including the complaints mechanism, is to be made available on request.[71] 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.[72]

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

i Data protection policy

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

ii Cookie policy

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

iii Complaints mechanism

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

iv Contracts with data intermediaries

Contracts with data intermediaries should set out clearly the intermediaries' obligations and include clauses relating to the retention period of the data and its 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.

70 Section 12(c) of the PDPA.

71 Section 12(d) of the PDPA.

72 Sections 11(4), 11(5) of the PDPA.

v Employee data protection policy

Employees should be notified about 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 DISCOVERY AND DISCLOSURE

The data protection provisions under the PDPA do not affect any rights or obligations under other laws.[73] 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, use or disclose 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.[74] 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.[75] 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.[76]

73 Section 4(6) of the PDPA.

74 First Schedule, Part 3, Paragraph 3 of the PDPA.

75 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.

76 Section 10(4) of the PDPA.

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,[77] carrying out investigations (whether on its own accord or upon a complaint), giving directions to an organisation or a person to ensure compliance with certain provisions in the PDPA,[78] and imposing financial penalties for contravention of certain provision in the PDPA.[79]

To enable the PDPC to carry out its functions effectively, it has been entrusted with broad powers of investigation,[80] 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 of up to S$1 million.[81] The PDPC may also in its discretion compound the offence.[82] Certain breaches can attract penalties of up to three years' imprisonment.[83] 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.[84] 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.[85]

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.[86]

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.

77 Section 48H of the PDPA.

78 See Section 48I. The PDPC has the power to give directions in relation to Parts III, IV, V, VI, VIA, VIB, IX and Section 48B(1) of the PDPA.

79 See Section 48J. The PDPC has the power to impose financial penalty for contraventions of Parts III, IV, V, VI, VIA, VIB, IX and Section 48B(1) of the PDPA.

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

81 Section 48J of the PDPA.

82 Section 55 of the PDPA.

83 Section 56 of the PDPA.

84 Section 52 of the PDPA.

85 Section 53 of the PDPA.

86 Section 48R of the PDPA.

ii Recent enforcement cases

The PDPC published 29 enforcement decisions in 2021, and 17 decisions from January 2022 to July 2022. 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 2021 and the first half of 2022 set out the PDPC's typical mix of behaviour remedies combined with financial penalties, including the following.

Vhive (June 2022)

The PDPC issued a fine of S$22,000 to Vhive[87] for failing to put in place reasonable security arrangements to protect the personal data of 186,281 of its customers (their names, addresses, email addresses, telephone numbers, hashed passwords and customer IDs) in its possession from a ransomware attack. Among other things, the PDPC found that Vhive failed to have a security maintenance policy or conduct any security reviews, and even though Vhive outsourced all of its IT to an outside vendor, the relevant contract failed to stipulate clear written security maintenance and data protection requirements to the vendor.

Love Bonito (May 2022)

The PDPC imposed a fine of $24,000 on Love Bonito[88] for failing to put in place reasonable security to protect personal data in its possession. One of Love Bonito's IT systems was hacked, and the personal data of 5,5561 of its customers was accessed and exfiltrated by a malicious actor. In its decision, the PDPA identified a number of significant weaknesses in Love Bonito's host, network, remote access and webpage security, such as failing to follow a robust password policy (the password for the administrator account was 'ilovebonito88').

Toll Logistics (Asia) and others (May 2022)

The PDPC issued warnings to several organisations for breaches of the PDPA in relation to the transfer of employee's personal data to human resources software vendor in London. In its decision, the PDPC noted that the organisations were required to take appropriate steps to ensure that the personal data transferred out of Singapore via its human resource platform for storage in the European Economic Area would be protected to a standard comparable under the PDPA, before any transfer was made, but there was no evidence of any such steps having been taken.

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

87 Case No. DP-2013-B8138.

88 Case No. DP-1912-B5484.

may be taken for that contravention until after the right of appeal has been exhausted and the final decision is made.[89] 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.[90]

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

As noted above, organisations are subject to mandatory data breach notification obligations under the PDPA, if the breach is notifiable. Government sector regulators have also 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. Relatedly, several other amendments to the Personal Data Protection (Notification of Data Breaches) Regulations 2021 and Personal Data Protection Regulations 2021 took effect on 1 October 2021. These include clarifications as to what constitutes 'significant harm' for mandatory data breach reporting, defences for egregious mishandling of personal data and ways organisations may provide the business contact information of their Data Protection Officers.

ii Cybersecurity

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

In Singapore, the CMA and the Cybersecurity Act are the key pieces of legislation governing cybercrime and cybersecurity. The CMA is primarily focused on defining various cybercrime offences, including criminalising the unauthorised accessing[91] or modification of computer material,[92] use or interception of a computer service,[93] obstruction of use of a computer[94] and unauthorised disclosure of access codes.[95]

89 Section 48O of the PDPA.

90 Advisory Guidelines on Enforcement of the Data Protection Provisions issued by the PDPC on 21 April 2016 and revised on 1 February 2021 at Paragraph 36.3.

91 Sections 3 and 4 of the CMA.

92 Section 5 of the CMA.

93 Section 6 of the CMA.

94 Section 7 of the CMA.

95 Section 8 of the CMA.

The 2017 amendments to the CMA added the offences of obtaining or making available personal information that the offender believes was obtained through a computer crime,[96] and using or supplying software or other items to commit or facilitate the commission of a computer crime.[97]

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 (Commissioner) with broad authority, including the power to establish mandatory codes of practice and standards of performance for CII owners.

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

a the computer or system continues to be available and operational;

b the integrity of the computer or system is maintained; or

c the integrity and confidentiality of information stored in, processed by or transmitted through the computer or system is maintained.

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

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

The Cybersecurity Act represents a move away from sector-based regulation. The Act requires mandatory reporting to the Commissioner 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

96 Section 8A of the CMA.

97 Section 8B of the CMA.

establish a common and consistent national framework was the better option. However, sectoral regulators continue to play a part in regulation in this area. For example, in December 2018, MAS launched a S$30 million cybersecurity capabilities grant to enhance cybersecurity capabilities in the financial sector and assist financial institutions in developing local talent in the cybersecurity sector. The Infocomm Media Development Authority has also formulated codes of practice to enhance the cybersecurity preparedness for designated licensees. The codes are currently imposed on major internet service providers in Singapore for mandatory compliance.

X OUTLOOK

The amendments of the PDPA represent an important step in bringing Singapore's data privacy law in line with international standards, such as the GDPR. As outlined above, apart from consent given by an individual, organisations in Singapore now have more legal bases to collect, use or disclose personal data. In particular, the ability for organisations to deem consent by notification will give business more flexibility in managing and using the personal data collected, as organisations may not necessarily be able to foresee all purposes the data collected will be used for at the time of collection. At the same time, certain newly introduced elements, particularly the mandatory data breach notification, also serve to encourage accountability on the part of organisations in the handling of personal data.

In recent years, the PDPC has been increasing enforcement efforts and has begun actively enforcing breaches of the PDPA. With the increased maximum financial penalties, organisations should pay careful attention to their evolving legal obligations in the PDPA. Further, the rise in popularity of hybrid work presents new challenges and creates a more urgent need to strengthen digital defences and data security. In a sign that cybersecurity is likely to be an ongoing priority for the Singapore government, a comprehensive review of the Cybersecurity Act has been announced and new developments are anticipated.

Appendix 1

ABOUT THE AUTHORS

MARGARET HOPE ALLEN

Sidley Austin LLP

Margaret Hope Allen represents companies and board committees in internal investigations and whistleblower actions all over the world, often involving allegations of fraud and corruption. Margaret has represented companies in investigatory and enforcement proceedings by the Department of Justice, the Securities and Exchange Commission, the United States Air Force, and state regulatory agencies.

Margaret also represents individuals and corporations in complex disputes in international arbitration and in courts across the United States. Her extensive experience litigating class actions and multi-jurisdictional disputes spans all aspects of pleadings, discovery, trial, and appeal. She litigates all manner of high-risk business disputes, including those involving breach of contract, business torts, and securities claims.

In addition, Margaret represents public and private companies in high-stakes civil rights and employment cases, and advises on significant employment and anti-corruption matters in a myriad of contexts, including national and international corporate transactions and reorganisations.

In 2022, Margaret was ranked as a leading employment lawyer by *Chambers USA*, which noted that clients praise her for being 'both a tough negotiator and a calming influence on all parties', as well as 'extremely quick at responding and a very direct communicator'. Margaret has been named a 'Texas Rising Star' by *Texas Super Lawyers* from 2012–2018 and one of the top 50 Up-and-Coming Women in 2018.

YUET MING THAM

Sidley Austin LLP

Yuet Ming Tham is the global co-chair of the white collar: government litigation and investigations practice. She speaks fluent English, Mandarin, Cantonese and Malay and is admitted in New York, England and Wales, Hong Kong and Singapore. Yuet focuses on cross-border work, and in the context of privacy and cybersecurity she has led projects globally including setting up compliance hotlines and advising on relevant labour and privacy laws as well as on the implementation of the EU Whistleblower Protection Directive. Yuet has set up numerous data privacy programmes for clients across Asia Pacific, and these have included drafting SOPs, data transfer agreements and online data policies. She has deep experience in the area of crisis management including major breach incidents.

Yuet's multiple accolades include being named by *Global Investigations Review* 2021 in its 'Top 100 Women in Investigations' in the world; a leading lawyer in the *Women in Business Law Expert Guide* 2021; 'Dispute Resolution Star: White-collar' by *Benchmark Litigation Asia-Pacific*, 2019–2022; *Who's Who Legal: Thought Leaders – Global Investigations Review* 2019-2020 and *Who's Who Legal: Thought Leaders – Hong Kong* 2020; Emerging Markets 'Compliance & Investigations Lawyer of the Year' by *The Asian Lawyer*, and a top ranked lawyer since 2012 by *Chambers Global* and *Chambers Asia-Pacific* for corporate investigations/anti-corruption: international, where she was described as 'a trusted counsel . . . in relation to global investigations and compliance advice' and 'is frequently sought after by international corporations, who respect her experience and expertise in risk management'.

FARAAZ AMZAR

Sidley Austin LLP

Faraaz Amzar focuses his practice on defending corporate and individual clients in government enforcement actions, internal investigations and complex commercial litigation matters.

Prior to joining Sidley, Faraaz was a Magistrate of the State Courts of Singapore, where he handled a variety of civil cases (employment, construction, statutory harassment) and presided over 120 tribunal trials in the Employment Claims and Small Claims Tribunals. Faraaz was a Justices' Law Clerk at the Supreme Court of Singapore where he clerked for the Chief Justice and Judges of the Court of Appeal, High Court and Singapore International Commercial Court.

Faraaz earned his LLB (First Class Honors) from the National University of Singapore, where he was on the overall Dean's list for academic performance from 2014 to 2018 and was awarded best student in international commercial litigation (awarded by Thomson Reuters) and best student in family law (awarded by LexisNexis).

SIDLEY AUSTIN LLP

NEO Building
Rue Montoyer 51 Montoyerstraat
B-1000 Brussels
Belgium
Tel: +32 2 504 64 00
jquartilho@sidley.com

39/F Two International Finance Centre
Central
Hong Kong
Tel: +852 2509 7645 / 2509 7868 / 2509 7637
Fax: +852 2509 3110
yuetming.tham@sidley.com
linh.lieu@sidley.com
lester.fung@sidley.com

ISBN 978-1-80449-116-4