The Privacy, Data Protection and Cybersecurity Law Review

Editor
Alan Charles Raul

Law Business Research

The Privacy, Data Protection and Cybersecurity Law Review

The Privacy, Data Protection and Cybersecurity Law Review
Reproduced with permission from Law Business Research Ltd.

This article was first published in The Privacy, Data Protection and Cybersecurity Law Review - Edition 1
(published in November 2014 – editor Alan Charles Raul).

For further information please email
Nick.Barette@lbresearch.com

The Privacy, Data Protection and Cybersecurity Law Review

Editor

Alan Charles Raul

Law Business Research Ltd

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 INTERNATIONAL 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

www.TheLawReviews.co.uk

PUBLISHER
Gideon Roberton

BUSINESS DEVELOPMENT MANAGER
Nick Barette

SENIOR ACCOUNT MANAGERS
Katherine Jablonowska, Thomas Lee, James Spearing

ACCOUNT MANAGER
Felicity Bown

PUBLISHING COORDINATOR
Lucy Brewer

MARKETING ASSISTANT
Dominique Destrée

EDITORIAL ASSISTANT
Shani Bans

HEAD OF PRODUCTION AND DISTRIBUTION
Adam Myers

PRODUCTION EDITOR
Timothy Beaver

SUBEDITOR
Janina Godowska

MANAGING DIRECTOR
Richard Davey

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

www.TheLawReviews.co.uk

ISBN 978-1-909830-28-8

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

ACKNOWLEDGEMENTS

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

ASTREA

BALLAS, PELECANOS & ASSOCIATES LPC

BOGSCH & PARTNERS LAW FIRM

DUNAUD CLARENC COMBLES & ASSOCIÉS

ELIG, ATTORNEYS-AT-LAW

JONES DAY

KIM & CHANG

NNOVATION LLP

NOERR

PINHEIRO NETO ADVOGADOS

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SYNCH ADVOKAT AB

URÍA MENÉNDEZ ABOGADOS, SLP

WINHELLER RECHTSANWALTSGESELLSCHAFT MBH

CONTENTS

EDITOR'S PREFACE

The first edition of *The Privacy, Data Protection and Cybersecurity Law Review* appears at a time of extraordinary policy change and practical challenge for this field of law and regulation. In the United States, massive data breaches have vied with Edward Snowden and foreign state-sponsored hacking to make the biggest impression on both policymakers and the public. In Europe, the 'right to be forgotten', the draconian new penalties proposed in the draft Data Protection Regulation and the Snowden leaks, have significantly altered the policy landscape.

Moreover, the frenetic conversion of the global economy to an increasingly digital, internet-driven model is also stimulating a rapid change in privacy, data protection and cybersecurity laws and regulations. Governments are playing catch-up with technological innovation. It is reported that half the world's population will be online by 2016 and the economies of emerging nations (except, perhaps, in Africa) are being developed directly through electronic commerce rather than taking the intermediate step of industrial growth as Western economies did. Growth and change in this area is accelerating, and rapid changes in law and policy are to be expected.

In France, whistle-blowing hotlines are meticulously regulated, but now, in certain key areas like financial fraud or corruption, advance authorisation for the hotlines is automatic under a 2014 legal amendment. In Singapore, 2014 saw the first enforcement matter under that country's Personal Data Protection Act – imposing a financial penalty on a company that sent unsolicited telemarketing messages. In Russia, a new 2014 'forced localisation' law requires data about Russians to be stored on servers in-country rather than wherever the data can be most efficiently managed and processed, and jurisdictions around the world have debated enacting such proposals. Interestingly, while notice of the location of the relevant servers must be provided to the Russian data protection authority, it is not clear whether the law prohibits personal data to be simultaneously stored both in-country and in foreign servers.

The European Union continues to seek to extend its model for data protection regulation around the world by deeming only countries that adopt the 'omnibus' legislative approach of the EU to be 'adequate' for data protection purposes. The EU model is not being universally endorsed, even outside the US and the Asia and Pacific

Economic Cooperation (APEC) economies. But nonetheless, the EU's constraints on international data transfers have substantially inhibited the ability of multinational companies to move personal data around the world efficiently for business purposes. In particular, conflicts with the US abound, exacerbated by the Snowden leaks regarding US government surveillance. One of the primary methods by which such EU–US data flows are facilitated, the US–EU Safe Harbor regime, has come under attack from EU parliamentarians who believe that such information will not be as carefully protected in the US and could become more susceptible to surveillance, despite the comparable surveillance authorities of EU intelligence agencies.

While policy conflicts over data protection conflicts appeared to be moderating before the Snowden leaks, afterwards, officials around the world professed to be so shocked that governments were conducting surveillance against possible terrorists that they appear to have decided that US consumer companies should pay the price. Some observers believe that digital trade protection, and the desire to promote regional or national 'clouds', play some role in the antagonism leveled against US internet and technology companies.

The fact that the US does not have an omnibus data protection law, and thus does not have a top-level privacy regulator or coordinator, means that it has been difficult for the US to explain and advocate for its approach to protecting personal information. This has allowed the EU to fill a perceived policy void by denying mutual recognition to US practices, and to impose significant extraterritorial regulatory constraints on American and other non-European businesses.

Nevertheless, it cannot be denied that privacy enforcement in the US is distinctly more aggressive and punitive than anywhere else in the world, including the EU. Substantial investigations and financial recoveries have been conducted and achieved by the Federal Trade Commission (which has comprehensive jurisdiction over consumer data and business practices), 50 state attorneys general (who have even broader jurisdiction over consumer protection and business acts and practices), private class action lawyers who can bring broad legal suits in federal and state courts, and a plethora of other federal and state agencies, such as the Consumer Financial Protection Bureau, the Federal Communications Commission, the Department of Health and Human Services (for medical and health-care data), the Department of Education, the Securities and Exchange Commission and various banking and insurance agencies.

In sum, there are no shortage of privacy regulators and enforcers in the US, Europe, and Asia. Enforcement in South America, as well as Africa and the Middle East appears to be developing more slowly.

Trumping many other privacy concerns, however, is the spate of data breaches and hacking that have been epidemic and part of public discourse in the years following California's enactment of the first data breach notification law in 2003. While the US appears (as a consequence of mandatory reporting) to be suffering the bulk of major cyberattacks – on retailers, financial institutions and companies with intellectual property worth stealing by foreign competitors or governments – it is also true that the US is leading the rest of the world on data breach notification laws and laws requiring that companies adopt affirmative data security safeguards for personal information.

For corporate and critical infrastructure networks and databases, the US has also led the way with a presidential executive order and the Cybersecurity Framework

developed by the National Institute of Standards and Technology in the US Department of Commerce. The United Kingdom has also been a leader in this area, developing the UK CyberEssentials programme, which will soon include an option for companies to be certified as compliant with the programme's cybersecurity standards. The EU Parliament has also enacted cybersecurity directives, and the EU's European Network and Information Security Agency has provided extensive and expert analysis, guidance and recommendations for promoting cybersecurity for EU-based organisations.

Despite attempts to implement baselines for cyber safeguards, it appears that no one is immune and no organisation is sufficiently protected to have any confidence that it can avoid being the victim of successful cyberattacks, particularly by the sophisticated hackers employed by state sponsors, organised crime, social hacktivists or determined, renegade insiders (like Snowden). Government agencies and highly resourced private companies have been unable to prevent their networks from being penetrated, and sometimes are likely to identify 'advanced persistent threats' months after the malware has begun executing its malicious purposes. This phenomenally destructive situation cannot obtain, and presumably some more effective solutions will have to be identified, developed and implemented. What those remedies will be, however, is not at all clear as 2014 yields to 2015.

In the coming year, it would seem plausible that there could be efforts at international cooperation on cybersecurity as well as cross-border enforcement against privacy violators. Enforcers in the EU, US and among the APEC economies, may increasingly agree to work together to promote the shared values embodied in the 'fair information practices principles' that are common to most national privacy regimes. In early 2014, a step in this direction was taken when APEC and the European Union's Article 29 Working Party (on Data Protection) jointly released a framework by which international data transfers could be effectuated pursuant to the guidelines of both organisations.

Challenges and conflicts will continue to be factors with respect to: assurances of privacy protection 'in the cloud'; common understandings of limits on and transparency of government access to personal data stored either in the cloud, or by internet companies and service providers; differences about how and when information can be collected in Europe (and perhaps some other countries) and transmitted to the US for civil discovery and law enforcement or regulatory purposes; freedom of expression for internet posts and publications; the ability of companies to market on the internet and to track – and profile – users online through cookies and other persistent identifiers; and the deployment of drones for commercial and governmental data acquisition purposes.

The biggest looming issue of them all, however, will likely be 'big data'. This is a highly promising practice – based on data science and analytics – that collects and uses enormous quantities of disparate (and often unstructured) data, and applies creative new algorithms enabled by vastly cheaper and more powerful computer power and storage. Big data can discover helpful new patterns and make useful new predictions about health problems, civic needs, commercial efficiencies, and yes, consumer interests and preferences.

The potential social utility of big data has been unequivocally acknowledged by the US administration as well as by the key policymakers in the EU. But, big data challenges the existing privacy paradigm of notice and disclosure to individuals who are then free to

make choices about how and when their data can be used and collected. Many existing and proposed applications of big data only work if the vast stores of data collected by today's companies can be maintained and analysed irrespective of purpose limitations. Such limitations may have been relevant (and disclosed) at the point of collection, but no longer address the value of the data to companies and consumers who can benefit from big data applications. Numerous highly thoughtful reports by policymakers in the US and EU have noted concerns about the possibility that unfettered big data applications could result in hidden discrimination against certain demographic groups that might be difficult to identify and correct; or could result in undue profiling of individuals that might inhibit their autonomy, limit their financial, employment, insurance or even serendipitous choices, or possibly somehow encroach on their personal privacy (to the extent that otherwise aggregate or anonymous data can be re-identified).

This publication arrives at a time of enormous ferment for privacy, data protection and cybersecurity. Readers are invited to provide any suggestions for the next edition of this compendium, and we look forward to seeing how the many fascinating and consequential issues addressed here will evolve or develop in the next year.

Alan Charles Raul
Sidley Austin LLP
Washington, DC
November 2014

Chapter 16

SINGAPORE

Yuet Ming Tham, Ijin Tan and Teena Zhang[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) Register 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.

---

1 Yuet Ming Tham is a partner and Ijin Tan and Teena Zhang are associates at Sidley Austin LLP.

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

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 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 will 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

The Singapore courts saw its first PDPA-related enforcement matter in August 2014 where a tuition agency and its director were fined a total of S$80,000 for sending unsolicited telemarketing messages in contravention of the DNC Register provisions. At the time of writing, there have not yet been any enforcement matters related to the data protection provisions at the point of publication.

There appears to have been an increase in the number of cyberattacks and security breaches in the past year. In December 2013, Standard Chartered Bank's server at a printing facility was hacked into, causing client information relating to 647 of its private banking clients to be stolen. The theft was only discovered after the authorities analysed the laptop of a suspected hacker for separate offences. There were also been several high-profile hack attacks on various government websites by 'hacktivist' group, Anonymous, in late 2013. The latest security breach on a government website was discovered in June 2014, where the personal data of 1,560 residents was compromised via the government's online portal, SingPass. SingPass allows Singapore residents to access some 340 online services, including the filing of income taxes and checking balances of the government-run compulsory savings plan. It was discovered that the passwords to some of the accounts had been illegally reset, and some of the accounts had been fraudulently used to apply for employment passes.

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

3 Ibid.

(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, it is 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.[4]

Also, 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.[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] 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]

---

4 Ibid.

5 Paragraph 5.28, PDPC Advisory Guidelines on Key Concepts in the Personal Data Protection Act, issued on 24 September 2013 and revised on 16 May 2014 (the 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.

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.

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 of 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]

In order 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 health-care sectors. In September 2014, the PDPC released the revised Selected Topics Advisory Guidelines, which includes a new chapter on photography. While the advisory guidelines are not legally binding, they provide helpful insight and guidance into the problems particular to each sector.

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 withdrawn at any time with reasonable notice. 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

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.

consent to the collection, use and disclosure of an individual's personal data for the purposes of the other organisations within the corporate group.[22]

Purpose limitation[23]

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[24]

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 and includes suggestions on the layout, language and placement of notifications.[25]

Access and correction[26]

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 request.[27]

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 they are able to provide a response to the request.[28]

Accuracy[29]

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.

22 Para 12.32, PDPA Key Concepts Guidelines.

23 Section 18 of the PDPA.

24 Section 20 of the PDPA.

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

26 Sections 21 and 22 of the PDPA.

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

28 Para 15.34, PDPA Key Concepts Guidelines.

29 Section 23 of the PDPA.

Protection[30]

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.[31]

Retention limitation[32]

An organisation may not retain such personal data for longer than is reasonable for the purpose for which it was collected and 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[33]

An organisation may not transfer personal data to a country or territory outside of 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[34]

An organisation is obliged to implement necessary policies and procedures in compliance with the PDPA, and 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 and 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 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 of time so that the individual becomes identifiable, then the organisation would be found to have collected personal data.

30 Section 24 of the PDPA.

31 See discussion in paragraphs 17.1–17.3, PDPC Key Concepts Guidelines.

32 Section 25 of the PDPA.

33 Section 26 of the PDPA.

34 Section 11 and 12 of the PDPA.

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.[35] Where cookies used for behavioural targeting involve the collection and use of personal data, the individual's consent is required.[36] Express consent may not be necessary in all cases; consent may be reflected when an individual has configured his 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.[37] It is not clear how practicable this would be in practice; a cloud-computing service may adopt multi-tenancy and data commingling architectures in order 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 the personal data for protection, and ensure it has established platforms with a robust security and governance framework.

As regards to social media, one issue arises where personal data is disclosed on social networking platforms, and which 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 was publicly available at the point of collection, the organisation will be able to use and disclose the same without consent.[38]

iv Specific regulatory areas

Minors

The PDPA does not contain special protection for minors (under 21 years of age).[39] However, the Advisory Guidelines noted 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, the organisation should obtain consent from the minor's parents or legal guardians on their behalf.[40] The Education Guidelines[41] provide further guidance

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

36 Ibid., Paragraph 7.11.

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

38 Para 12.55, PDPA Key Concepts Guidelines.

39 Section 8.1, PDPA Selected Topics Guidelines.

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

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

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[42] 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 their 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.

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[43] 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 Register, the obligations only apply to senders of messages or calls to Singapore numbers, and 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 an employee of the purposes of the collection, use and disclosure of their personal data and obtain their consent.

---

42 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 advisors; 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.

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

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 its collection, use and disclosure.[44] 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 in the company intranet.

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

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.

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.[47]

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.[48] 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.[49]

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

45 Para 1(f) Second Schedule, Para 1(f) Third Schedule and para 1(h) Fourth Schedule of the PDPA.

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

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

48 Regulation 9 of the PDP Regulations.

49 Regulation 10 of the PDP Regulations.

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;[50] 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.[51]

V COMPANY POLICIES AND PRACTICES

Organisations are obliged to develop and implement policies and practices necessary for the organisation to meet its obligations under the PDPA.[52] Organisations must also develop a complaints mechanism[53] and communicate to their staff the policies and practices they have implemented.[54] Information on the policies and practices, including the complaints mechanism, is to be made available on request.[55] 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 make his business contact information publicly available.[56]

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 the 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.

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

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

52 Section 12 (a) of the PDPA.

53 Section 12(b) of the PDPA.

54 Section 12(c) of the PDPA.

55 Section 12(d) of the PDPA.

56 Section 11(4) of the PDPA.

ii Cookie policy

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

iii Complaints mechanism

The organisation should develop a process to receive and respond to complaints it receives, and may 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 its 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, so for 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 is 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.[57] 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.

57 Section 4(6) of the PDPA.

The PDPA has carved out specific exceptions in respect of investigations and proceedings. Thus, an organisation may collect data about an individual without their consent where such collection is necessary for any investigation or proceedings, so as not to compromise the availability or accuracy of the personal data.[58] 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.[59] These exceptions, however, do not extend to internal audits or investigations. Nevertheless, it may be argued that consent from the employees are not required as such audits would fall within the purpose of managing or terminating the relationship.[60] Employees may be notified of such potential purposes 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 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.[61]

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

The PDPC is the key agency responsible for administering and enforcing the PDPA. Its role includes, among other things, reviewing complaints from individuals[62], carrying out investigations (whether on its on accord or upon a complaint), prosecuting and adjudicating on certain matters arising out of the PDPA.[63]

To enable the PDPC to carry out its functions effectively, it has been entrusted with broad powers of investigation,[64] including the power to require organisations to produce documents or information and the power to enter premises with or without a warrant in order to carry out a search. In certain circumstances, the PDPC may obtain a search and seizure order from the state courts to search the premises and take possession of any material that appears to be relevant to the 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

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

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

60 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.

61 Section 10(4) of the PDPA.

62 Section 28 of the PDPA.

63 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.

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

the breach, and impose financial penalties up to S$1 million.[65] The PDPC may also in its discretion compound the offence.[66] Certain breaches can attract penalties of up to three years' imprisonment.[67] 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 consent or connivance, or is attributable to his neglect.[68] 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.[69]

Directions issued by the PDPC may be appealed to be heard before the Appeal Committee. Thereafter, any appeals against decision 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.[70]

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

ii Recent enforcement cases

As the provisions of the PDPA have only recently come into force, there has only been one enforcement case brought before the Singapore State Courts. On 4 June 2014, the PDPC brought charges against a tuition agency and its director for 37 counts of contravening the DNC provisions relating to the organisation's obligation to check the DNC Registry before sending telemarketing messages. The defendants pleaded guilty to 13 of the 37 counts and were fined a total of S$80,000 by the state courts.

However, since the DNC provisions came into effect on 2 January 2014, the PDPC has conducted investigations into 3,700 valid complaints from members of the public against 630 organisations, from sectors such as property, tuition and insurance.[71] Two organisations have had their offences compounded for amounts between S$500 S$1,000. About 380 organisations that had received isolated complaints, were issued warning notices regarding the sending of unsolicited telemarketing messages.

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, no private action

65 Section 29 of the PDPA.

66 Section 55 of the PDPA.

67 Section 56 of the PDPA.

68 Section 52 of the PDPA.

69 Section 53 of the PDPA.

70 Section 35 of the PDPA.

71 https://www.pdpc.gov.sg/docs/default-source/media/media-release---pdpc-takes-action-against-tuition-agency-and-organizations-(230514).pdf?sfvrsn=2 (current as at 4 September 2014).

against the organisation may be taken until after the right of appeal has been exhausted and the final decision is made.[72]

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 breach

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, the Monetary Authority of Singapore (MAS) has 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 of the incident.

ii Cybersecurity

Singapore is not a signatory to the Council of Europe's Convention on Cybercrime.
In Singapore, the Computer Misuse and Cybersecurity Act (the Cybersecurity Act) is the key legislation governing cybercrime and cybersecurity. In particular, it regulates:

a unauthorised access to or modification of computer material;[73]
b unauthorised use or interception of a computer service;[74] and
c unauthorised disclosure of access codes.[75]

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.[76] In particular, the Minister of Home Affairs may direct entities to take such pre-emptive measures as necessary to prevent, detect or counter

72 Section 32 of the PDPA.

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

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

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

76 This would include the energy, finance and banking, ICT, security and emergency services, transportation, water, government and health-care sectors.

any cybersecurity threat posed to the national security, essential services or defence of Singapore or foreign relations of Singapore.[77]

X OUTLOOK

Despite the lengthy period given to organisations to ready themselves for the new data protection regime, many smaller businesses may not have adopted the necessary measures prescribed by the PDPA. For example, it has been observed that merchants continue to collect cardholders' personal data via a practice known as 'double-swiping', where credit cards are swiped a second time for marketing purposes such as loyalty programmes.[78] Such practices contravene the PDPA as personal data beyond what is necessary for payment is being collected without consent of the customer. In the year ahead, we can expect the PDPC to adopt a fairly active and aggressive approach in enforcing the requirements of the data protection provisions, as it did in respect of the DNC Register provisions.

Following the release of new advisory guidelines in the education, social services and health-care sectors in September 2014, we expect to see increased surveillance of data privacy practices in these sectors in the coming year. It is also anticipated that further guidance would be issued so as to offer clarity on the interpretation and application of the PDPA. Given that the PDPA is still at a nascent stage, it is unlikely that there will be any major amendments to the same especially since it is deliberately drafted broadly. There may, however, be some fine-tuning of the obligations as they relate to specific sectors or where there is a need to keep up with new technological challenges. Cloud computing and social media in particular, present unique challenges to data protection principles.

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

78 www.straitstimes.com/news/singapore/more-singapore-stories/story/credit-card-swiped-second-time-its-against-privacy-law-2 (accessed on 9 September 2014)

Appendix 1

ABOUT THE AUTHORS

YUET MING THAM

Sidley Austin LLP

Yuet Ming Tham is a partner in Sidley Austin's Hong Kong office. 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 Japan, China, Australia, Korea, India, Indonesia, Thailand, Taiwan, Hong Kong, Malaysia, Singapore and the Philippines.

Yuet is named as a leading lawyer in *Chambers Asia Pacific* in four categories, as well as being recognised in *IFLR 1000* and *Asia Pacific Legal 500*. In 2014, she was the only lawyer awarded the 'Client Choice' award by International Law Office for white-collar crime practice in Hong Kong.

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

IJIN TAN

Sidley Austin LLP

Ijin Tan is an associate in Sidley's Singapore office. Her practice focuses on data privacy law, cross-border compliance and investigations. She frequently works with clients on cross-border data privacy issues, data protection and compliance, and has assisted clients in setting up a whistle-blowing programme. Her clients include international corporations in industries such as pharmaceutical, medical devices, oil and gas, electronics, and

commodities on matters. Additionally, Ijin has significant experience in drafting internal policies such as dawn raid and business conduct policies for multinational corporations, and routinely conducts training for senior management. Ms Tan is fluent in English and Mandarin.

TEENA ZHANG
Sidley Austin LLP
Teena Zhang is an associate in Sidley's Singapore office. She has experience in data privacy law, compliance, data protection and cybersecurity law. Her practice also includes advising clients in the energy and resources industry, and has worked on infrastructure projects and transactions. Prior to joining Sidley, Teena spent three years with an international law firm in Melbourne and Perth, Australia, before moving to Iraq to work with an Iraqi law firm. She is fluent in English and Mandarin.

SIDLEY AUSTIN LLP
39/F Two International Finance Centre
Central
Hong Kong
Tel: +852 2509 7888
Fax: +852 2509 3110
yuetming.tham@sidley.com

Level 31, Six Battery Road
Singapore 049909
Tel: +65 6230 3900
Fax: +65 6230 3939
yuetming.tham@sidley.com
ijin.tan@sidley.com
teena.zhang@sidley.com

www.sidley.com