THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

FIFTH EDITION

Editor
Alan Charles Raul

THE LAWREVIEWS

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

Fifth Edition

Reproduced with permission from Law Business Research Ltd
This article was first published in October 2018
For further information please contact Nick.Barette@thelawreviews.co.uk

Editor
Alan Charles Raul

THE LAWREVIEWS

PUBLISHER
Tom Barnes

SENIOR BUSINESS DEVELOPMENT MANAGER
Nick Barette

BUSINESS DEVELOPMENT MANAGERS
Thomas Lee, Joel Woods

SENIOR ACCOUNT MANAGER
Pere Aspinall

ACCOUNT MANAGERS
Jack Bagnall, Sophie Emberson, Katie Hodgetts

PRODUCT MARKETING EXECUTIVE
Rebecca Mogridge

RESEARCHER
Keavy Hunnigal-Gaw

EDITORIAL COORDINATOR
Thomas Lawson

HEAD OF PRODUCTION
Adam Myers

PRODUCTION EDITOR
Anna Andreoli

SUBEDITOR
Martin Roach

CHIEF EXECUTIVE OFFICER
Paul Howarth

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

www.TheLawReviews.co.uk

ISBN 978-1-912228-62-1

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

ACKNOWLEDGEMENTS

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

ALLENS

ASTREA

BOGSCH & PARTNERS LAW FIRM

BTS&PARTNERS

JUN HE LLP

KOBYLAŃSKA & LEWOSZEWSKI KANCELARIA PRAWNA SP J

M&M BOMCHIL

MÁRQUEZ, BARRERA, CASTAÑEDA & RAMÍREZ

MATHESON

MATTOS FILHO, VEIGA FILHO, MARREY JR E QUIROGA ADVOGADOS

NNOVATION LLP

NOERR

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SK CHAMBERS

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

WALDER WYSS LTD

WINHELLER RECHTSANWALTSGESELLSCHAFT MBH

CONTENTS

Chapter 1 GLOBAL OVERVIEW 1
Alan Charles Raul

Chapter 2 EUROPEAN UNION OVERVIEW 5
William RM Long, Géraldine Scali, Francesca Blythe and Alan Charles Raul

Chapter 3 APEC OVERVIEW 40
Ellyce R Cooper and Alan Charles Raul

Chapter 4 ARGENTINA 53
Adrián Lucio Furman, Mercedes de Artaza and Francisco Zappa

Chapter 5 AUSTRALIA 64
Michael Morris

Chapter 6 BELGIUM 77
Steven De Schrijver

Chapter 7 BRAZIL 98
Fabio Ferreira Kujawski and Alan Campos Elias Thomaz

Chapter 8 CANADA 109
Shaun Brown

Chapter 9 CHINA 125
Marissa (Xiao) Dong

Chapter 10 COLOMBIA 136
Natalia Barrera Silva

Chapter 11 GERMANY 146
Olga Stepanova

Chapter 12 HONG KONG 154
Yuet Ming Tham

Chapter 13 HUNGARY 169
Tamás Gödölle

Chapter 14 INDIA 189
Aditi Subramaniam and Sanuj Das

Chapter 15 IRELAND 206
Anne-Marie Bohan

Chapter 16 JAPAN 220
Tomoki Ishiara

Chapter 17 MALAYSIA 237
Shanthi Kandiah

Chapter 18 MEXICO 251
César G Cruz-Ayala and Diego Acosta-Chin

Chapter 19 POLAND 266
Anna Kobylańska, Marcin Lewoszewski, Maja Karczewska and Aneta Miśkowiec

Chapter 20 RUSSIA 277
Vyacheslav Khayryuzov

Chapter 21 SINGAPORE 287
Yuet Ming Tham

Chapter 22 SPAIN 304
Leticia López-Lapuente and Reyes Bermejo Bosch

Chapter 23 SWITZERLAND 317
Jürg Schneider, Monique Sturny and Hugh Reeves

Chapter 24 TURKEY 338
Batu Kınıkoğlu, Selen Zengin and Kaan Can Akdere

Chapter 25 UNITED KINGDOM 350
William RM Long, Géraldine Scali and Francesca Blythe

Chapter 26 UNITED STATES 376
Alan Charles Raul and Vivek K Mohan

Appendix 1 ABOUT THE AUTHORS 405
Appendix 2 CONTRIBUTING LAW FIRMS' CONTACT DETAILS 419

Chapter 17

MALAYSIA

Shanthi Kandiah[1]

I OVERVIEW

The Personal Data Protection Act 2010 (PDPA), which came into force on 15 November 2013, sets out a comprehensive cross-sectoral framework for the protection of personal data in relation to commercial transactions.

The PDPA was seen as a key enabler to strengthen consumer confidence in electronic commerce and business transactions given the rising number of cases of credit card fraud, identity theft and selling of personal data without customer consent. Before the PDPA, data protection obligations were spread out among certain sectoral secrecy and confidentiality obligations, while personal information was primarily protected as confidential information through contractual obligations or civil actions for breach of confidence.

The PDPA imposes strict requirements on any person who collects or processes personal data (data users) and grants individual rights to 'data subjects'. Enforced by the Commissioner of the Department of Personal Data Protection (the Commissioner), it is based on a set of data protection principles akin to that found in the Data Protection Directive 95/46/EC of the European Union (EU)[2] and, for this reason, the PDPA is often described as European-style privacy law. An important limitation to the PDPA is that it does not apply to the federal and state governments.[3]

The processing of information by a credit reporting agency is also exempted from the PDPA. In the past, credit reporting agencies did not fall under the purview of any regulatory authority in Malaysia, drawing heavy criticism for inaccurate credit information reporting. The Credit Reporting Agencies Act 2010, which came into force on 15 January 2014, now provides for the registration of persons carrying on credit reporting businesses under the regulatory oversight of the Registrar Office of Credit Reporting Agencies, a division under the Ministry of Finance, which is charged with developing a regulated and structured credit information sharing industry.

---

1 Shanthi Kandiah is a partner at SK Chambers. She was assisted in writing this chapter by Aida Harun and Carmen Koay, associates at SK Chambers.

2 The EU Data Protection Directive 95/46/EC has now been replaced with the EU General Data Protection Regulation, which came into force on 25 May 2018.

3 There is some ambiguity about which public entities fall within this definition. It does not appear that agencies and statutory bodies established under Acts of Parliament or state enactments to perform specific public functions, such as Bank Negara Malaysia (BNM), the Employees Provident Fund, the Securities Commission Malaysia and the Companies Commission of Malaysia, fall within the scope of this exemption.

i Cybersecurity

The PDPA enumerates the security principle as one of its data protection principles. Under this principle, an organisation must ensure both technical and organisational security measures are well in place to safeguard the personally identifiable information that it processes. The ISO/IEC 27001 Information Security Management System (ISMS), an international standard, which deals with information technology systems risks such as hacker attacks, viruses, malware and data theft, is the leading standard for cyber risk management in Malaysia.

Sectoral regulators such as BNM and the Securities Commission Malaysia have also been actively tackling issues relating to cybersecurity in relation to their relevant sectors by issuing guidelines and setting standards for compliance (discussed in Section IX).

The intersection between privacy and cybersecurity also manifests in the extent of the tolerance for government surveillance activity: the PDPA does not constrain government access to personal data, as discussed in Section VI. The reasons given to justify broad government access and use include national security, law enforcement and the combating of terrorism.

II THE YEAR IN REVIEW

The most significant development this year that has affected and will continue to affect the legal landscape in Malaysia is the installation of a new federal government following the outcome of the Malaysian general elections held on 9 May 2018. The new Minister of Communications and Multimedia (Mr Gobind Singh Deo) has signalled firm commitment to enforcement against data breaches, ordering follow-up action on cases of personal data breaches that had received significant media attention.

To date, the Commission's enforcement actions tend towards enforcement of straightforward breaches. As at June 2018, there are now at least five enforcement cases that have resulted in conviction by the court and at least another eight cases that are expected to be tried in court. A majority of the convictions are for the offence of processing personal data without a certificate of registration.[4]

Several organisations in the following sectors have also received inspection visits from the Commissioner's office: utility, insurance, healthcare, banking, education, direct selling, tourism and hospitality, real estate and services (retail and wholesale). Section 101 of the PDPA gives the Commissioner power to inspect the personal data systems in corporations with a view to making recommendations on compliance. The organisation is given limited notice of the pending visit. If an organisation fails to make the necessary improvements post-inspection, this could lead to criminal enforcement action under the PDPA. An inspection visit from the Commissioner's staff will entail a detailed review of the following areas:

a personal data collection forms and privacy notice;

b internal standard operating procedures for personal data management within the organisation;

c person in charge of personal data management within the organisation and his or her awareness of the legal requirements; and

4 Section 16(4) of the PDPA.

d compliance with the seven data protection principles in the PDPA.

Complaints remain the primary trigger for the investigation and enforcement activities of the Commissioner. As at June 2018, the Commissioner has received over 700 official complaints since the coming into force of the law. Unsurprisingly, a majority of complaints relate to processing of data in the electronic environment.[5]

Cybersecurity issues have also received significant media attention as Malaysian companies were not spared in the global ransomware attacks, such as the WannaCry cyberattack in 2017. Currently, Malaysia does not have a specific law addressing cybersecurity-related offences. Enforcement agencies, such as the National Cybersecurity Agency (NCSA), have to rely on existing legislation, such as the Communications and Multimedia Act 1998 (CMA), the Defamation Act 1957 and the Sedition Act 1948, to combat cyberthreats.[6]

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

The PDPA is a comprehensive data protection legislation containing seven data protection principles, including the general principle establishing the legal requirements for processing personal data (e.g., with consent or in compliance with the legal requirements), notice (internal privacy notices for employees and external notices for consumers), choice, disclosure, data security, integrity and retention, and rights of access. Failure by an organisation to observe these principles is an offence.[7] The Personal Data Protection Standards 2015, which came into force on 23 December 2015 (the Standards) are considered the 'minimum' standards to be observed by companies in their handling of personal data of customers and employees, and failure to implement them carries criminal sanctions.

The PDPA also sets up a co-regulatory model that emphasises the development of enforceable industrial codes of practice for personal data protection against the backdrop of the legal requirements of the government. Codes of Practice that have been approved and registered by the Commissioner include the Personal Data Protection Code of Practice for the Utilities Sector (Electricity),[8] the Personal Data Protection Code of Practice for the Insurance/Takaful Industry[9] and the Personal Data Protection Code of Practice for the Banking and Financial Sector.[10] Additional codes of practice – one for the communications sector and one for legal practitioners – are also expected to be introduced sometime this year.

As the Codes set sector-specific prescriptions, it is likely that these will set the expected standards for the specific sector, over and above the Standards. Non-compliance with the codes will also carry penal consequences.[11]

5 Meeting with officers of the Commissioner at the Personal Data Protection Department in Putrajaya on 9 July 2018.

6 See Section IX.i.

7 Section 5(2) of the PDPA.

8 With effect from 23 June 2016.

9 With effect from 23 December 2016.

10 With effect from 19 January 2017.

11 Section 29 of the PDPA.

Personal data

Three conditions must be fulfilled for any data to be considered as 'personal data' within the ambit of the PDPA.[12]

First, the data must be in respect of commercial transactions. 'Commercial transactions' is defined under the PDPA as transactions of a commercial nature, whether contractual or not, and includes any matter relating to the supply or exchange of goods or services, agency, investments, financing, banking and insurance.[13] There is some ambiguity as to whether an activity must have a profit motivation to be considered a commercial transaction.

Second, the information must be processed or recorded electronically or recorded as part of a filing system.

Third, the information must relate directly or indirectly to a data subject who is identifiable from the information or other information in the possession of the data user. A central issue for the application of the PDPA is the extent to which information can be linked to a particular person. If data elements used to identify the individual are removed, the remaining data becomes non-personal information, and the PDPA will not apply.[14]

Sensitive personal data

Sensitive personal data is defined as any personal data consisting of information as to:

a the physical or mental health or condition of a data subject;

b his or her political opinions;

c his or her religious beliefs or other beliefs of a similar nature;

d the commission or alleged commission by him or her of any offence; or

e any other personal data as the minister responsible for personal data protection (currently the Minister of Communications and Multimedia) may determine.[15]

Sensitive personal data may only be processed with the explicit consent of the data subject and in the limited circumstances set out in the PDPA.[16]

Application of the PDPA

The PDPA applies to any person who processes or has control over the processing of any personal data in respect of commercial transactions.

'Processing' has been defined widely under the PDPA to cover activities that are normally carried out on personal data, including collecting, recording or storing personal data, or carrying out various operations such as organising, adapting, altering, retrieving, using, disclosing and disseminating the data. The prevailing view with respect to social media companies which have established a presence in Malaysia (for example through opening a branch office in Malaysia), is that they will be regarded as a data user and be subject to the PDPA for any data which they process in Malaysia (such as the personal data of their employees). Data processed wholly outside of Malaysia may not fall within the purview of the PDPA. In this connection, there appears to be some doubt about the application of

12 Section 2 of the PDPA.

13 Section 2 of the PDPA.

14 See also Section 45(1)(c) of the PDPA.

15 Section 2 of the PDPA.

16 Section 40(1) of the PDPA.

the PDPA to social media companies where it concerns data of users of social media if the interpretation taken is that this data is not being processed by the branch office in Malaysia or that no equipment in Malaysia is being used to process the data, except for the purpose of transit through Malaysia.[17]

A further point to note is that the PDPA only regulates personal data in the context of commercial transactions. As such, there is also some ambiguity as to whether a nominal user of social media (i.e., for recreational and social use) would enjoy the protection offered by the PDPA.

Most of the obligations under the PDPA apply to a 'data user' (i.e., 'a person who either alone or jointly in common with other persons processes any personal data or has control over or authorises the processing of any personal data, but does not include a data processor').

A 'data processor' who processes personal data solely on behalf of a data user is not bound directly by the provisions of the PDPA.

ii General obligations for data users

Registration

The Personal Data Protection (Class of Data Users) Order 2013 lists 11 categories of data users who have to be registered with the Commissioner. The categories are:

a banking and finance;
b insurance;
c telecommunications;
d utilities;
e healthcare;
f hospitality and tourism;
g education;
h real estate and property development;
i direct selling;
j services (e.g., legal, accountancy, business consultancy, engineering, architecture, employment agencies, transportation); and
k retail and wholesale.

The list of data users was expanded in 2016 to include two additional sectors: pawnbroking and money lending.[18] Failure to register by these categories of data users is an offence.[19]

Purpose limitation

A data user may not process personal data unless it is for a lawful purpose directly related to the activity of the data user, the processing is necessary and directly related to the purpose, and the personal data are adequate and not excessive in relation to that purpose.

The data subject must also consent to the processing of the personal data unless the processing is necessary for specific exempted purposes.[20]

17 Section 2(2) of the PDPA

18 Personal Data Protection (Class of Data Users) (Amendment) Order 2016, which came into effect on 16 December 2016.

19 Section 16(4) of the PDPA.

20 Section 6(2) of the PDPA.

Consent

The PDPA does not define 'consent'; nor does it prescribe any formalities in terms of the consent. However, the Personal Data Protection Regulations 2013 (the Regulations) provide that the data user must keep a record of consents from data subjects. The Regulations further provide that the Commissioner or an inspection officer may require production of the record of consents. It places the burden of proof for consent squarely on the data user.

Helpfully, the Personal Data Protection Code of Practice for the Utilities Sector (Electricity) provides examples of consent, whether express or implied, that must be recorded or maintained by the data user. These examples include:

a signatures, or a clickable box indicating consent;
b deemed consent;
c verbal consent; and
d consent by conduct or performance.

Consent is deemed given by way of conduct or performance if the data subject does not object to the processing; the data subject voluntarily discloses its personal data; or the data subject proceeds to use the services of the data user.

Verbal consent should be recorded digitally or via a written confirmation that consent was given.

Explicit consent

Regarding explicit consent, the Personal Data Protection Code of Practice for the Utilities Sector (Electricity) provides the following examples: where the data subject provides his or her identification card to be photocopied or scanned; where the data subject voluntarily provides the sensitive personal data; and verbal statements that have been recorded or maintained.

Notification

Data users are obliged to notify individuals of their purposes for the collection, use and disclosure of personal data on or before such collection, use or disclosure. For example, where a data user intends to use personal information collected for a different purpose, such as marketing communications, the data user must provide the affected individuals with the choice to disagree with the purpose before doing so.

Disclosure

Data users shall not disclose personal data for any purpose other than that for which the data was disclosed at the time of collection, or for a purpose directly related to it; or to any party other than a third party of the class notified by the data user without a data subject's consent.[21]

Retention

Personal data should not be kept longer than necessary. Retention policies must take into account any relevant requirements imposed by applicable legislation. However, the Standards appear to impose organisational requirements that may be challenging for organisations to

21 If a data user is found guilty of disclosing personal data without the consent of the data subject, he or she may be liable to a 300,000-ringgit fine or two years' imprisonment, or both.

comply with. Personal data collection forms are required to be destroyed within a period of 14 days, unless the forms can be said to have some 'legal value' in connection with the commercial transaction. It is unlikely that this time frame would be feasible for most organisations.

A record of destruction should be properly kept and be made available when requested by the Commissioner.

Data subjects' rights

A data subject has various rights to his or her personal data kept by data users. These are:

a the right of access to personal data;[22]
b the right to correct personal data;[23]
c the right to withdraw consent;[24]
d the right to prevent processing likely to cause damage or distress;[25] and
e the right to prevent processing for purposes of direct marketing.[26]

iii Technological innovation

In general, the regulatory framework has not developed specific rules (outside the application of the seven principles in the PDPA) to deal with data privacy issues created by cookies, online tracking, cloud computing, the internet of things or big data.

Government efforts appear to be focused on positioning the country appropriately to benefit from these innovations. For example, the Ministry of Science, Technology and Innovation has unveiled the National Internet of Things Strategic Roadmap (the Roadmap). Under the Roadmap, a centralised regulatory and certification body will be established to address privacy, security, quality and standardisation concerns.

iv Specific regulatory areas

There are special confidentiality rules that apply to data in specific sectors, such as the banking and financial institutions sectors, the healthcare sector as well as the telecommunications and multimedia sectors. However, these rules do not comprehensively cover all aspects of data protection in the comprehensive manner addressed by the PDPA, which tracks the information life cycle from its collection and use through to its storage, destruction or disclosure.

Minors

The PDPA does not contain specific protection for minors (below the age of 18). Section 4 of the PDPA states that for minors, the guardian or person who has parental responsibility for the minor shall be entitled to give consent on behalf of the minor.

22 Section 30 of the PDPA.
23 Section 34 of the PDPA.
24 Section 38 of the PDPA.
25 Section 42 of the PDPA.
26 Section 43 of the PDPA.

Financial institutions

A banker's duty of secrecy in Malaysia is statutory as is clearly provided under Section 133(1) of the Financial Services Act 2013 (FSA). The duty is not absolute.[27] Section 153 of the FSA provides the legal basis for BNM to share a document or information on financial institutions with an overseas supervisory authority.[28]

The Guidelines on Data Management and MIS[29] Framework issued by BNM sets out high-level guiding principles on sound data management and MIS practices that should be followed by financial institutions. It is noteworthy that boards of directors and senior management are specifically entrusted with the duty to put in place a corporate culture that reinforces the importance of data integrity.

Healthcare

The Medical Act 1971 is silent on the duty of confidentiality. The Confidentiality Guidelines issued by the Malaysian Medical Council in October 2011 after the PDPA was enacted are the most comprehensive articulation of the confidentiality obligation of health professionals.

Multimedia and telecommunications

The General Consumer Code of Practice (GCC), developed by the Communications and Multimedia Consumer Forum of Malaysia, sets out a number of consumer protection principles, one of which is the protection of consumers' personal information (quite similar in scope to the seven PDPA principles) for the telecommunications and multimedia sectors. The GCC binds all licensed service providers under the CMA and all non-licensed service providers who are members of the Consumer Forum.[30]

Direct selling

The PDPA prescribes direct sellers as one of the 11 classes of data users that must register with the Personal Data Protection Department.

The PDPA also gives consumers the right to request in writing that the direct seller stop or not begin processing their personal data. Failure to cease using personal data for direct marketing purposes after a data subject has objected could make the offender liable for a fine of up to 200,000 ringgit, imprisonment for up to two years, or both.

IV INTERNATIONAL DATA TRANSFER AND DATA LOCALISATION

Section 129(1) of the PDPA states that a company may only transfer personal data out of Malaysia if the country is specified by the Minister of Communications and Multimedia Malaysia and this is then published in the Gazette. The Commissioner had issued a Public Consultation Paper[31] entitled Personal Data Protection (Transfer of Personal Data To Places Outside Malaysia) Order 2017 (the Proposed Order 2017), which seeks feedback from the public on the Commissioner's draft whitelist of countries to which the personal data

27 Schedule 11 of the FSA sets out a list of permitted disclosures.

28 See also Section 165 of the Islamic Financial Services Act 2013.

29 Management Information System.

30 The Malaysian Communications and Multimedia Content Code also sets out privacy related restrictions.

31 (PCP) No. 1/2017.

originating in Malaysia may be freely transferred without having to rely on exemptions provided by Section 129(3) of the PDPA. The places identified in the Proposed Order 2017 are as follows: European Economic Area member countries, the United Kingdom, the United States, Canada, Switzerland, New Zealand, Argentina, Uruguay, Andorra, the Faroe Islands, Guernsey, Israel, the Isle of Man, Jersey, Australia, Japan, Korea, China, Hong Kong, Taiwan, Singapore, the Philippines and Dubai International Financial Centre.

As at June 2018, the Proposed Order 2017 has yet to be gazetted. Until it comes into effect, to transfer data outside the country, organisations will have to rely on the exemptions set out in Section 129(3) PDPA, which include:

a where the data subject has consented to the transfer;

b where the transfer is necessary for the performance of a contract between the data subject and the data user;

c where the transfer is necessary to protect the vital interests of the data subject; and

d where the data user has 'taken all reasonable precautions and exercised all due diligence' to ensure that the personal data will not be processed in the recipient country in a way that would be a contravention of the PDPA.

Unlike EU law, Malaysian law does not require transfer contracts to be made for the benefit of third parties. Malaysia also has a doctrine of privity of contract that prevents enforcement of third-party benefits by data subjects.

V COMPANY POLICIES AND PRACTICES

Organisations are under the obligation to implement policies and enforce certain practices to ensure their compliance with the PDPA.

i Data protection officers

The requirements for a data protection officer are not mandated under the law. However, the Commissioner's Proposal Paper (No. 2/2014), Guidelines on Compliance with Personal Data Protection 2010, makes a clear proposal for every organisation to establish responsibility for protection of personal data at the highest level and to designate an officer for this responsibility. The officer's primary responsibility will be to ensure that all policies, procedures, systems and operations are aligned with the PDPA. There is, however, no requirement for a senior management position such as a chief privacy officer.

In addition, the proposed Guidelines appear to place the responsibility for protection of personal data at the highest level, which would appear to suggest that privacy should be a board level issue.

ii Online privacy policies

It is not uncommon for an organisation's privacy policy to be used as a privacy notice. Privacy policies are sometimes used as a privacy notice in lieu of developing a separate document.

iii Internal privacy policies for employees' rights and responsibilities

The notice and choice principle requires an employer to inform the employee of the nature of the information collected; whether the information will be shared with a third party; and that he or she has the right to access the information collected.

iv Requirement for data privacy due diligence and oversight over third parties

The Standards require data users, in discharging the security principle, to bind third parties contractually to ensure the safety of personal data from misuse, loss, modification, unauthorised access and disclosure. Some organisations do take the additional step of reserving audit rights over third parties processing personal data of their behalf, but this is not currently mandated.

v Written information security plan

The Regulations require that data users develop and implement a security policy for their companies. This security policy must comply with standards established by the Commissioner from time to time.[32] Some of the more prescriptive standards for implementation are the standards stipulating that the transfer of personal data through removable media devices (e.g., USB thumb drives) and cloud computing services (e.g., Dropbox and Google Drive) is no longer permitted, unless authorised in writing by the 'top management' of the company.

Even when permitted, each transfer of personal data via such a removable media device must be recorded. Additionally, data users are required to record access to personal data, and to make the records available to the Commissioner upon request.

vi Incident response plan

Data breach management and incident response plans have not been mandated by the Commissioner.

VI DISCOVERY AND DISCLOSURE

The data protection provisions under the PDPA do not affect any rights and obligations under other laws. There is a clear exemption for disclosure of personal data for a purpose other than the purpose for which data was collected where the disclosure is necessary for the purpose of preventing or detecting a crime, or for the purpose of investigations.

In this regard, Malaysian legislation (including the PDPA) tends to provide authorities with extensive powers of search and seizure, including powers to search without a warrant. This power arises where the delay in obtaining a search warrant is reasonably likely to adversely affect investigation, or where evidence runs the risk of being tampered with, removed or destroyed.

Section 263(2) of the CMA is particularly noteworthy. Internet service providers as licensees under the CMA must comply with the Malaysian Communications and Multimedia Commission or any other authorities that make a written request for their assistance in preventing an offence or the attempt of any crime listed under Malaysian law.

Section 263(2) is broad enough to permit authorities to gain access to telecommunications information such as contact information and content of communications.

32 The Personal Data Protection Standards 2015.

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

The Commissioner has been entrusted with certain powers under the PDPA to enforce the PDPA. It has conferred powers to carry out inspections and investigations on data users, whether or not these are initiated by any complaints received from the public. The powers of the Commissioner include:

a conducting inspections on data users' personal data systems;
b publishing reports that set out any recommendations arising from the inspections; and
c serving enforcement notices on data users for a breach of any of the provisions of the PDPA, and directing data users to take (or refrain from taking) specified steps to ensure that they comply with the PDPA.

The Commissioner's authorised public officers also have various powers of enforcement under the PDPA, including:

a conducting investigations on the commission of any offence under the PDPA;
b conducting searches and seizure of data users' computerised data, documents, equipment, systems and properties, with or without a warrant;
c requiring the production of computers, books, accounts, computerised data or other documents kept by data users; and
d arresting without warrant any person who the authorised public officer reasonably believes has committed or is attempting to commit an offence under the PDPA.

It is worth highlighting a provision that is now commonplace in Malaysian legislation (including the PDPA) that provides that where an offence is committed by a body corporate, its director, chief executive officer, chief operating officer, manager, secretary or other similar officer, the entity or person may be deemed to have committed the offence unless it, he or she can establish that there was no knowledge of the contravention, and that it, he or she has exercised all reasonable precautions and due diligence to prevent the commission of the offence.[33]

ii Recent enforcement cases

In early 2018, an online employment agency was convicted and fined 10,000 ringgit for processing personal data without a certificate of registration. This is the second case involving an employment agency in the services sector that has led to a conviction.[34]

iii Private litigation

The PDPA does not provide for a statutory civil right of action for breach of any of the provisions of the PDPA. An aggrieved individual can nevertheless still pursue a civil action under common law or tort against a data user who has misused the individual's personal data.

33 Section 133(1) of the PDPA.

34 http://www.pdp.gov.my/index.php/my/pusat-media/berita/989-pengguna-data-yang-telah-dikenakan-tindakan-di-bawah-akta-perlindungan-data-peribadi-2010-akta-709.

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

The PDPA applies to all activities relating to the collection, use and disclosure of personal data in Malaysia. As such, it will also apply to foreign entities processing such data in Malaysia regardless of whether they have an actual physical presence in Malaysia. The PDPA does not apply to personal data that is processed outside Malaysia, unless the data is intended to be further processed in Malaysia.

IX CYBERSECURITY AND DATA BREACHES

Statistics from Cybersecurity Malaysia for 2018 – MyCERT Incident Statistics – indicate that from January to May 2018 alone there have been over 2,713 reports on cyber-related incidents.[35] This figure does not include those cases that go unreported almost daily, as there is no requirement to report breaches to the authorities or to customers.

The National Cybersecurity Policy is Malaysia's integrated cybersecurity implementation strategy to ensure the critical national information infrastructure (CNII) is protected to a level that is commensurate with the risks faced. Cutting across government machineries, the implementation has drawn in various ministries and agencies to work together to create a CNII that is secure, resilient and self-reliant. Implementation of this scheme has involved certification of CNIIs by Cybersecurity Malaysia to be ISMS-compliant. Other initiatives include Cyber999 Help Centre, which is a service operated by the Malaysian Computer Emergency Response Team (MyCERT) for internet users to report or escalate computer security incidents.

BNM has also issued a circular on 'Managing Cybersecurity Risks', under which financial institutions are required to adhere to the 'Minimum Measures To Mitigate Cyberthreats'. Measures include measures to:

a assess the implementation of multi-layered security architecture;

b ensure security controls for server-to-server external network connections;

c ensure the effectiveness of the monitoring undertaken by Security Operation Centre to view security events, including incidents of all security devices and critical servers on a 24/7 basis; and

d subscribe to reputable threat intelligence services to identify emerging cyberthreats, uncover new cyberattack techniques and provide counter measures.

The Securities Commission Malaysia has also issued its Guidelines on Management of Cyber Risk,[36] which sets out a framework to address cybersecurity resilience for capital market participants' management of cybersecurity risks.

i Cyberlaws

In contrast to the comprehensive approach of the PDPA, Malaysia's cyberlaws are scattered across various pieces of legislation. Presently, the key provisions of Malaysia's cyberlaws are as follows.

35 www.mycert.org.my/statistics/2018.php.

36 With effect from 31 October 2016.

CMA

Offences under the CMA include:

a the offence of the use of network facilities or network services by a person to transmit any communication that is deemed to be offensive and that could cause annoyance to another person;[37]

b the offence of using an apparatus or device without authority;[38]

c the offence of improper use of network facilities or network services – such as annoying, abusive, threatening, harassing or obscene communications – emails (spamming), SMS or MMS website content publishing;[39]

d the offence of interception and disclosure of communications;[40] and

e the offence of damage to network facilities.[41]

Other cyberoffences include:

a cyberpornography and exploitation of children;[42]

b online sedition and internet defamation;[43]

c misuse of computers;[44]

d prostitution and other illegal cybersexual activities; and

e cyberterrorism.[45]

ii Laws to facilitate prosecutions of internet-based offences

A noteworthy development in Malaysian law was the introduction of Section 114A into the Evidence Act 1950, which came into force on 31 July 2012. Under the new Section 114, a person is deemed to be a publisher of a content if it originates from his or her website, registered networks or data-processing device of an internet user unless he or she proves the contrary.

iii Laws to promote tracking transactions conducted on the internet

Examples of laws that provide for tracking and recording transactions conducted on the internet include the Cyber Centre and Cyber Cafe (Federal Territory of Kuala Lumpur) Rules 2012 and the Consumer Protection (Electronic Trade Transactions) Regulations 2012. The former requires any person operating a cybercafé and cybercentre to maintain a customer

37 Section 233(1)(a) of the CMA.

38 Section 231 of the CMA.

39 Section 233 of the CMA.

40 Section 234 of the CMA.

41 Section 235 of the CMA.

42 Sections 292, 293 and 294 of the Penal Code, Section 5 of the Film Censorship Act 2002 and Section 31 of the Child Act 2001.

43 Sections 3 and 4 of the Sedition Act 1948, Section 211 (prohibition on provision of offensive content) and Section 233 (improper use of network facilities or network service) of the CMA.

44 Section 3 (unauthorised access to computer materials), Section 4 (unauthorised access with intent to commit or facilitate commission of further offence), Section 5 (unauthorised modification of contents of any computer) and Section 6 (wrongful communications) of the Computer Crimes Act 1997.

45 The Penal Code contains provisions that deal with terrorism that may apply to cyberterrorism, such as Chapter VIA Sections 130B–130T (incorporated into the Penal Code on 6 March 2007).

entry record and a record of computer usage for each computer, whereas the latter require online business owners and operators to provide their full details and terms of conditions of sale, to rectify errors and maintain records.

X OUTLOOK

We expect to see more enforcement actions by the Commissioner in the coming year, particularly given the focus of the new Minister on enforcement of data breaches. Having said that, we expect to see the Commission continue to pursue its 'audit' type regulation (as opposed to prosecution) via inspection visits and enforcement notices as a means of instilling awareness amongst data users on their data protection obligations.

The Cambridge Analytica scandal in April 2018 received wide media coverage in Malaysia and is likely to have led to elevated awareness and concern among data subjects in Malaysia on their privacy rights, including the extent of use of their personal data by social media companies. This is said to be reflected through the high number of complaints from the public received by the office of the Commissioner this year. In light of this, it is possible that we will see more legal developments to regulate the internet and social media. Any ambiguity about the application of the PDPA to social media companies should be resolved as this is likely to be a recurring theme for user distress over data protection in the near future.

Compliance with the General Data Protection Regulation (GDPR), which came into force on 25 May 2018, is a topic we expect to see proactively addressed by Malaysian corporations that collect and process data of EU residents (such as customers, permanent residents, visitors and expatriates) given its extraterritorial reach and the potentially hefty fines that can be imposed due to breach.[46] The GDPR's prescriptions on organisational and technical measures to protect personal data are likely to influence Malaysian standard setting as well. For example, the office of the Commissioner has indicated that following the GDPR's lead, data breach notification is likely to be made compulsory in Malaysia.[47] A blanket requirement to report every breach could be excessively onerous. A threshold such as 'a real risk of serious harm' should accompany such a requirement (which would most certainly cover identity theft). In these cases, the breach notification should be made to the consumer. Alternatively, and instead of a mandatory requirement, Parliament may wish to consider explicitly recognising breach notification as a mitigation point in enforcement proceedings. This would not just address considerations on fairness to the consumer, but provide organisations with the incentive to advise consumers of breaches, as well as the flexibility to evaluate their position.

46 Maximum fine that can be imposed under the GDPR is 4 per cent of worldwide total annual turnover, or €20 million, whichever is higher.

47 Meeting with officers of the Commissioner at the Personal Data Protection Department in Putrajaya on 9 July 2018.

Appendix 1

ABOUT THE AUTHORS

SHANTHI KANDIAH

SK Chambers

Shanthi Kandiah founded SK Chambers with the goal of creating a stand-alone regulatory firm that services individuals and entities involved at all levels of the regulatory scheme. Today, SK Chambers does just that – it is focused on delivering legal services in competition law, the full spectrum of multimedia laws, privacy and data protection matters, and anti-bribery and corruption laws, as well as capital market laws and exchange rules.

Shanthi Kandiah regularly advises many corporations in sectors such as media and telecommunications, FMCG, construction and credit reporting on privacy and data protection matters, including the following: compliance strategies that prevent and limit risk; managing risks through contracts with customers and suppliers; data protection and cyberrisk due diligence in relation to acquisitions, dispositions and third-party agreements; crisis management when a data breach occurs; investigations management – when faced with regulatory action for data security breaches; and data transfers abroad – advising on risks and issues.

She holds an LLM and a postgraduate diploma in economics for competition law, both from King's College London.

SK CHAMBERS

9B Jalan Setiapuspa
Bukit Damansara
50490 Kuala Lumpur
Malaysia
Tel: +60 3 2011 6800
Fax: +60 3 2011 6801
sk@skchambers.co
www.skchambers.co

ISBN 978-1-912228-62-1