THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

EIGHTH EDITION

Editor
Alan Charles Raul

THE LAWREVIEWS

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

EIGHTH EDITION

Reproduced with permission from Law Business Research Ltd
This article was first published in October 2021
For further information please contact Nick.Barette@thelawreviews.co.uk

Editor
Alan Charles Raul

THE LAWREVIEWS

PUBLISHER
Clare Bolton

HEAD OF BUSINESS DEVELOPMENT
Nick Barette

TEAM LEADERS
Joel Woods, Jack Bagnall

BUSINESS DEVELOPMENT MANAGERS
Rebecca Mogridge, Katie Hodgetts, Joey Kwok

RESEARCH LEAD
Kieran Hansen

EDITORIAL COORDINATOR
Georgia Goldberg

PRODUCTION AND OPERATIONS DIRECTOR
Adam Myers

PRODUCTION EDITOR
Anne Borthwick

SUBEDITOR
Jonathan Allen

CHIEF EXECUTIVE OFFICER
Nick Brailey

Published in the United Kingdom
by Law Business Research Ltd, London
Meridian House, 34–35 Farringdon Street, London, EC4A 4HL, UK

www.TheLawReviews.co.uk

ISBN 978-1-83862-810-9

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

ACKNOWLEDGEMENTS

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

ADVOKAADIBÜROO NORDX LEGAL

ALLENS

ANJIE LAW FIRM

ASTREA

AZEVEDO SETTE ADVOGADOS

BOGSCH & PARTNERS LAW FIRM

BOMCHIL

BTS & PARTNERS

CLEMENS

CTSU, SOCIEDADE DE ADVOGADOS, SP, RL, SA

GREENBERG TRAURIG LLP

K&K ADVOCATES

LEE, TSAI & PARTNERS

NOERR

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SK CHAMBERS

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

WALDER WYSS LTD

WINHELLER ATTORNEYS AT LAW & TAX ADVISORS

CONTENTS

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 Thong Xin Lin and Nimraat Kaur.

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.

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 the Central Bank of Malaysia (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, (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

Earlier this year, the Prime Minister of Malaysia Tan Sri Muhyiddin Yassin launched the MyDIGITAL initiative – a new and comprehensive approach designed to anchor the country's digital economy by year 2030. The Malaysian Digital Economy Blueprint (Blueprint) sets out the efforts and initiatives to deliver the MyDIGITAL initiative. The Blueprint includes initiatives to strengthen the data protection framework, notably a review of the PDPA.

Prior to this, in year 2020, the Minister of Communications and Multimedia announced that public consultations will be held to discuss possible amendments to the PDPA. The Minister further stated that the Communications and Multimedia Ministry had identified gaps within the PDPA when compared to personal data protection legislation in ASEAN member nations, Japan, South Korea and the European Union's General Data Protection Regulation (GDPR).[4] In February 2020, the Commissioner issued Public Consultation Paper No. 01/2020 on the Review of Personal Data Protection Act 2010 (Act 709) (the PDPA Consultation Paper). Among other things, the PDPA Consultation Paper sought views and comments from the public on a total of 22 issues including imposition of direct obligation on data processors, right to data portability, reporting of data breach incidents, privacy by design, and processing personal data in cloud computing. There has been no reported development in relation to the PDPA Consultation Paper.

In light of the coronavirus (covid-19) pandemic, the Commissioner issued an advisory on the collection, processing and retention of personal data by businesses permitted to operate during the conditional movement control order period (the Advisory), following its approval in a Special Ministerial Committee Meeting on the Implementation of the MCO held on 21 May 2020. As businesses were required to collect the name and phone numbers

4 https://www.malaymail.com/news/malaysia/2020/02/12/minister-govt-to-consult-public-on-amendments-to-personal-data-protection-l/1836984.

of visitors or customers in the event that contact tracing becomes necessary, the Advisory provided guidance to business operators on the steps to be taken to ensure compliance with the PDPA in the course of collecting or processing such information.

To-date, the Commissioner's enforcement actions tend towards enforcement of straightforward breaches such as offences for processing personal data without a certificate of registration. As at July 2021, there are at least five enforcement cases that have resulted in conviction by the court. A majority of the convictions are for the offence of processing personal data without a certificate of registration.[5]

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

Cybersecurity issues have also received significant media attention during the covid-19 outbreak, where there was increased use of and reliance on technology as Malaysia faced a movement control order. A total of 4,615 cybersecurity incidents were reported between January to May 2021 with the three highest incidents reported being fraud, intrusion and malicious code.[6] Currently, Malaysia does not have a specific law addressing cybersecurity-related offences. Enforcement agencies, such as the National Cyber Security Agency, 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.[7]

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.[8] The Personal Data Protection Standards 2015 (the Standards),

5 Section 16(4) of the PDPA.
6 https://www.malaymail.com/news/malaysia/2021/06/02/minister-4615-cybersecurity-incidents-reported-in-malaysia-from-jan-may/1979083.
7 See Section IX.i.
8 Section 5(2) of the PDPA.

which came into force on 23 December 2015, 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:

a utilities sector (electricity);[9]
b insurance/*takaful* industry;[10]
c banking and financial sector;[11]
d licensees under the Communications and Multimedia Act 1998;[12] and
e Malaysian aviation sector.[13]

A code of practice for legal practitioners is also expected to be introduced.

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.[14]

Personal data

Three conditions must be fulfilled for any data to be considered as 'personal data' within the ambit of the PDPA.[15]

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.[16] 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.[17]

9 The Personal Data Protection Code of Practice for the Utilities Sector (Electricity) came into effect from 23 June 2016. The Personal Data Protection Code of Practice for the Utilities Sector (Electricity) Version 2.0 came into effect from 21 January 2020.
10 With effect from 23 December 2016.
11 With effect from 19 January 2017.
12 With effect from 23 November 2017.
13 With effect from 21 November 2017.
14 Section 29 of the PDPA.
15 Section 4 of the PDPA.
16 Section 4 of the PDPA.
17 See also Section 45(2)(c) of the PDPA.

Sensitive personal data

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

a his or her physical or mental health or condition;
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.[18]

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.[19]

Data user

'Data user' means a person who either alone or jointly or 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.[20] A data user under the PDPA is analogous to a data controller under EU laws.

Data processor

'Data processor' means any person, other than an employee of the data user, who processes the personal data solely on behalf of the data user, and does not process the personal data for his or her own purposes.[21] An example of a data processor would be a third-party cloud computing service provider.

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 that 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 that 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.

There appears to be some doubt about the application of 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

18 Section 4 of the PDPA.
19 Section 40(1) of the PDPA.
20 Section 4 of the PDPA.
21 Section 4 of the PDPA.

is being used to process the data, except for the purpose of transit through Malaysia.[22] 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 considering that the PDPA only regulates personal data in the context of commercial transactions.

Most of the obligations under the PDPA apply to a data user. 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 handlers

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 financial institution;
b insurance;
c communications;
d utilities;
e health;
f tourism and hospitality;
g education;
h real estate;
i direct selling;
j services (e.g., legal, accountancy, business consultancy, engineering, architecture, employment agencies, retail and wholesale); and
k transportation.

The list of data users was expanded in 2016 to include two additional sectors: pawnbrokers and moneylenders.[23] Failure to register by these categories of data users is an offence.[24]

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 or 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.[25]

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 consent obtained must be recorded and maintained properly by the data user. The

22 Section 2(2) of the PDPA.
23 Personal Data Protection (Class of Data Users) (Amendment) Order 2016, which came into effect on 16 December 2016.
24 Section 16(4) of the PDPA.
25 Section 6(2) of the PDPA.

Regulations further provide that the Commissioner or an inspection officer may require production of the record of consent. It places the burden of proof for consent squarely on the data user.

Some classes of data users may also refer to the codes of practice issued by the Commissioner for the respective classes of data users on this topic and it is noteworthy that the requirements vary depending on the Code of Practice. For example, the Personal Data Protection Code of Practice for the Utilities Sector (Electricity) Version 2.0 provides examples of consent, whether express or implied, that must be recorded or maintained by the data user which includes:

a signatures, or a clickable box indicating consent;

b verbal consent (verbal consent should be recorded digitally or via a written confirmation that consent was given); and

c consent by conduct or performance. Consent is considered as 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.

Explicit consent

As stated above, explicit consent is one of the basis for the processing of sensitive personal data.[26] The PDPA does not specify what amounts to explicit consent, although it is likely that the standard of obtaining such consent would be higher than obtaining consent per se. Certain classes of data users may refer to the codes of practice issued by the Commissioner for the respective classes of data users on this topic. For example, the Personal Data Protection Code of Practice for the Utilities Sector (Electricity) Version 2.0 provides the following examples of explicit consent: where the data subject signs or marks at the relevant part of the application form; where the data subject voluntarily provides the sensitive personal data to the data user such as submitting a copy of his identity card to obtain services from the data user; and the data subject provides verbal statements giving consent for the processing of sensitive personal data that have been recorded.

Notification

Data users are obliged to notify a data subject that, among others, their personal data is being processed by or on behalf of the data user, and the purposes for which the personal data is being or is to be collected and further processed. 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.[27]

26 Section 40(1) of the PDPA.

27 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.

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 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.

iii Data subject rights

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

a the right of access to personal data;[28]
b the right to correct personal data;[29]
c the right to withdraw consent;[30]
d the right to prevent processing likely to cause damage or distress;[31] and
e the right to prevent processing for purposes of direct marketing.[32]

Complaint

Under the PDPA, the data subject can make a written complaint to the Commissioner about an act, practice or request:

a specified in the complaint;
b engaged in by the data user specified in the complaint;
c that relates to personal data of which the individual is the data subject; and
d that may be in contravention of the PDPA including any codes of practice.[33]

Upon receiving a complaint, the Commissioner may choose to conduct an investigation in relation to the relevant data user to ascertain whether the act, practice or request specified in the complaint contravenes the PDPA.[34] In the event that the complainant withdraws the complaint, the Commissioner may carry out or continue an investigation where the Commissioner is of the opinion that it is in the public interest to do so.[35] The enforcement powers of the Commissioner are further discussed in Section VII below.

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

28 Section 30 of the PDPA.
29 Section 34 of the PDPA.
30 Section 38 of the PDPA.
31 Section 42 of the PDPA.
32 Section 43 of the PDPA.
33 Section 104 of the PDPA.
34 Section 105(1) of the PDPA.
35 Section 107 of the PDPA.

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

Generally, the PDPA does not contain specific protection for minors (below the age of 18). However, the Regulations provide that a data user must obtain consent from the parent, guardian or person who has parental responsibility on the data subject if the data subject is a minor. Further, as a 'relevant person' under the PDPA,[36] such parent, guardian or person who has parental responsibility is entitled to make a complaint, data access request or data correction request for the minor.

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.[37] 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.[38]

The Guidelines on Data Management and MIS[39] 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.

In January 2017, the Commissioner also released the Personal Data Protection Code of Practice for the Banking and Financial Sector.

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 (CFM), sets out a number of consumer protection principles, one of which is the protection of consumers' personal information (quite similar

36 Section 4 of the PDPA provides that in the case of a data subject who is below the age of 18 years, the 'relevant person' in relation to a data subject means the parent, guardian or person who has parental responsibility for the data subject.

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

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

39 Management Information System.

in scope to the seven PDPA principles) for the telecommunications and multimedia sectors.[40] The GCC binds all licensed service providers under the CMA and all non-licensed service providers who are members of the CFM.[41]

Direct selling

The PDPA prescribes direct sellers as one of the 13 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.

v 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.

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[42] 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 originating in Malaysia may be freely transferred without having to rely on exemptions provided by Section 129(3) of the PDPA. As at July 2021, the Proposed Order 2017 has yet to be gazetted.

The PDPA Consultation Paper issued by the Commissioner in early 2020 indicates that the Commissioner is considering restructuring the provision of Section 129 and to remove the issuance of whitelist in Section 129. Until any changes on this come into effect, to transfer data outside the country, organisations will have to rely on the exemptions set out in Section 129(3) of the 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

40 The GCC is currently under review and a public consultation paper was released for the revised GCC from 3 March 2020 until 16 April 2020. As of September 2020, it was reported that CFM has been working with Malaysian Communications and Multimedia Commission and is in the process of tightening up the provisions of the GCC to ensure that consumer rights are protected. In the revised GCC, it appears that the provision on protection of personal information has been omitted. In any event, it can be argued that the PDPA still applies to licensees of the CMA.

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

42 (PCP) No. 1/2017.

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 laws, 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

As data users, 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.[43] 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.

The appointment of a data protection officer is also one of the issues being considered under the PDPA Consultation Paper.

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

The notice and choice principle requires a data user to inform a data subject that, among others, their personal data is being processed. As an employer, a data user is required to inform the employee (as a data subject) of this. To the extent that a data user processes the personal data of any classes of data subjects, an internal corporate privacy policy should be in place to address such class of data subjects.

iv Data mapping over collection, use, sale of data, transfers, storage, etc.

There are no specific requirements relating to data mapping; however, a data user is required to ensure the requirements of the PDPA are complied with when processing personal data. For example, personal data must not be processed unless it is necessary for or directly related to the purpose in which it was collected.

43 The proposed Guidelines have not been formalised to date.

v Required transparency and disclosure practices

The disclosure principle requires a data user to not disclose personal data without the consent of the data subject except in specific circumstances prescribed under the PDPA.

Additionally, the Regulations require the data user to keep and maintain a list of disclosure to third parties in relation to personal data of the data subject that has been or is being processed by him or her.

vi Privacy impact assessments

Privacy impact assessments have not been mandated by the Commissioner.

vii Data subject opt-in, opt-out, access, deletion and portability rights

In addition to the need for consent, the Public Consultation Paper (No. 1/2014) titled the Guide to Dealing with Direct Marketing under the Personal Data Protection Act (PDPA) 2010 provides that an individual must be given the right to refuse the use of personal data for direct marketing.[44] In the case of direct marketing by electronic means, an opt-out right must be made available on every subsequent marketing message. The right of portability is not available under the PDPA.

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

The PDPA and 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 on their behalf, but this is not currently mandated.

ix Privacy by design

Privacy by design has not been mandated by the Commissioner.

x 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.[45] 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.

xi Incident response plan

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

44 The public consultation paper has not been formalised to date.

45 The Personal Data Protection Standards 2015.

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, for the purpose of investigations, or the disclosure was required or authorised by law or by the order of a court.

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, damaged 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 (MCMC) 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.

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

The Commissioner has been entrusted with certain powers under the PDPA to enforce the PDPA. It is 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 remedy the contravention of 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' computers, books, accounts, computerised data, or documents, containing or reasonably suspected to contain information relating to an offence as well as equipment, instruments or articles reasonably believed to furnish evidence of the commission of an offence, 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 also be deemed to have committed the offence unless it, he or

she can establish that there was no knowledge, consent or connivance of the contravention, and that it, he or she has exercised all reasonable precautions and due diligence to prevent the commission of the offence.[46]

Any person who is aggrieved by a decision of the Commissioner under the PDPA may appeal to the Appeal Tribunal by filing a notice of appeal with the Appeal Tribunal.[47]

ii Recent enforcement cases

In 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.[48]

In recent times, the Commissioner has been responding to allegations published in the media relating to the sale of customers' personal data to American entities. In October 2020, it was reported that the Commissioner had accepted the clarification from AirAsia Group Berhad (AirAsia) in relation to an allegation about the sale of customers' personal data by AirAsia to an American firm.[49] In November 2020, the Commissioner obtained clarification from the Muslim Pro application for similar reasons.[50] It appears that no further action was taken following the clarification provided.

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.

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

The PDPA applies to any person processing personal data in respect of commercial transactions where the person is established in Malaysia and the personal data is processed by that person or any other person employed or engaged by that establishment. Where the person is not established in Malaysia, the PDPA will still apply if such person uses equipment in Malaysia for processing the personal data in commercial transactions other than for the purposes of transit through Malaysia. As such, the PDPA will also apply to foreign entities processing personal data in Malaysia regardless of whether they have an actual physical presence in Malaysia provided such person falls within the aforementioned categories. The PDPA does not apply to personal data that is processed outside Malaysia, unless the data is intended to be further processed in Malaysia.

46 Section 133(1) of the PDPA.

47 The Personal Data Protection (Appeal Tribunal) Regulations 2021 which provides for the conduct of appeals before the Appeal Tribunal came into effect from 15 April 2021.

48 https://www.pdp.gov.my/jpdpv2/berita_terkini/pengguna-data-yang-telah-dikenakan-tindakan-di-bawah-akta-perlindungan-data-peribadi-2010-akta-709/.

49 https://www.pdp.gov.my/jpdpv2/berita_terkini/dakwaan-kumpulan-airasia-berhad-airasia-menjual-data-peribadi-pelanggannya-kepada-firma-amerika-syarikat/?lang=en.

50 https://www.pdp.gov.my/jpdpv2/berita_terkini/siaran-media-jpdp-dakwaan-penjualan-data-peribadi-pengguna-aplikasi-muslim-pro-kepada-tentera-amerika-syarikat/?lang=en.

IX CYBERSECURITY AND DATA BREACHES

The National Cyber Security Policy (NCSP) was formulated by the National Cyber Security Agency[51] based on a National Cyber Security Framework comprising legislation and regulatory, technology, public–private cooperation, institutional and international aspects. The NCSP seeks to address risks to the Critical National Information Infrastructure (CNII) comprising networked information systems of 10 critical sectors, and to ensure that the CNII is protected to a level that is commensurate to the risks faced. Implementation of this scheme has involved certification of CNIIs by Cybersecurity Malaysia as being ISMS-compliant. Other initiatives include the Cyber999 Help Centre, which is a service operated by the Cybersecurity Malaysia – Malaysian Computer Emergency Response Team (MyCERT) for internet users to report or escalate computer security incidents.

MyCERT incident statistics indicate that in 2020 there were a total of 10,790 reports on cyber-related incidents.[52] Statistics from January to May 2021 indicate that there have been approximately 4,615 reports on cyber-related incidents.[53] Cybersecurity Malaysia is a national body established to monitor national e-security, and comes under the purview of the Ministry of Science, Technology and Innovation. The above-mentioned figures do not include those cases that go unreported almost daily, as there is no requirement under the PDPA to report breaches to the authorities or to customers.

Though there is currently no data breach notification requirement under the PDPA, it is worth noting that one of the issues being considered under the review of the PDPA in the PDPA Consultation Paper is mandatory reporting of data breach incidents. Currently, financial service providers subject to the purview of the BNM may also be required to, among other things, notify the BNM immediately upon discovery of a breach where the breach is likely to pose reputational risk to financial service providers or a threat to public confidence and trust.[54]

The BNM issued the policy document on Risk Management in Technology (RMiT policy document) and Electronic Know-Your-Customer (e-KYC) (e-KYC policy document) on 19 June 2020 and 30 June 2020 respectively. The RMiT policy document, among others, sets out the board and senior management responsibilities, the responsibilities of the chief information security officer, the requirement for financial institutions to establish a robust framework for managing technology projects, the requirement to conduct due diligence on third-party service providers, the requirement to conduct risk assessment prior to conducting cloud services, and to provide adequate and regular technology and cybersecurity awareness training. The e-KYC policy document sets out the minimum requirements and standards a financial institution must observe in implementing e-KYC for the identification and verification of individuals.

51 NACSA was established in February 2017 and is the national lead agency for cybersecurity matters, with the objective of securing and strengthening Malaysia's resilience in facing threats of cyberattacks.

52 https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&id=2650ed29-88be-4cec-86cc-13f8e07ae228.

53 https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&id=01851697-c9a1-4775-ad39-7975d446dec6.

54 This is pursuant to the Management of Customer Information and Permitted Disclosures policy document issued by the BNM on 17 October 2017

The Securities Commission Malaysia also issued its Guidelines on Management of Cyber Risk,[55] which sets out, among others, roles and responsibilities of the board of directors and management in the oversight and management of cyber risk and cyber risk policies and procedures that should be developed and implemented by capital market entities.

i Cyber laws

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.

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;[56]

b the offence of using an apparatus or device without authority;[57]

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;[58]

d the offence of interception and disclosure of communications;[59] and

e the offence of damage to network facilities.[60]

Other cyber offences include:

a cyberpornography and exploitation of children;[61]

b online sedition and internet defamation;[62]

c misuse of computers;[63]

d prostitution and other illegal cyber sexual activities; and

e cyberterrorism.[64]

55 With effect from 31 October 2016.

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

57 Section 231 of the CMA.

58 Section 233 of the CMA.

59 Section 234 of the CMA.

60 Section 235 of the CMA.

61 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.

62 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.

63 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.

64 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).

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 114A, 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 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

The Commissioner continues to pursue its 'audit' type regulation (as opposed to prosecution) via inspection visits and enforcement notices as the primary means of instilling awareness among data users on their data protection obligations. The Commissioner's Advisory, in connection with the conditional movement restriction order, again signalled the 'audit approach' as the Commissioner communicated its intention to carry out monitoring from time to time to assess level of compliance.

Although prospects to review the PDPA appear promising with the issuance of the PDPA Public Consultation Paper in 2020 and coupled with the government's initiative to enhance the nation's data protection laws in accordance with the My Digital Blueprint issued earlier this year, it remains to be seen whether any headway will be made on this topic as to date, there has been no reported developments on the process of amending the PDPA.

Over and above the amendments proposed in the Public Consultation paper which is largely focused on strengthening an organisation's accountability when handling personal data, it should be noted that the MyDigital Initiative also views a facilitative and robust legislative and regulatory framework as a critical enabler for the digital economy. In this regard it will be interesting to see if there might be a broadening of the scope of amendments (such as those seen in Singapore), to include recalibration towards meaningful consent and the introduction of new exceptions for the collection use and disclosure of personal data. These enhancements would be timely and will better enable organisations to take on challenges in the face of rapidly evolving technology and business landscapes.

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. She 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 cyber risk 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.

Shanthi Kandiah 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

an LBR business

ISBN 978-1-83862-810-9