

THE PRIVACY, DATA
PROTECTION AND
CYBERSECURITY
LAW REVIEW

FOURTH EDITION

Editor
Alan Charles Raul

THE LAWREVIEWS

THE PRIVACY, DATA
PROTECTION AND
CYBERSECURITY
LAW REVIEW

FOURTH EDITION

Reproduced with permission from Law Business Research Ltd
This article was first published in December 2017
For further information please contact Nick.Barette@thelawreviews.co.uk

Editor
Alan Charles Raul

THE LAWREVIEWS

PUBLISHER
Gideon Robertson

SENIOR BUSINESS DEVELOPMENT MANAGER
Nick Barette

BUSINESS DEVELOPMENT MANAGERS
Thomas Lee, Joel Woods

ACCOUNT MANAGERS
Pere Aspinall, Sophie Emberson,
Laura Lynas, Jack Bagnall

PRODUCT MARKETING EXECUTIVE
Rebecca Mogridge

RESEARCHER
Arthur Hunter

EDITORIAL COORDINATOR
Gavin Jordan

HEAD OF PRODUCTION
Adam Myers

PRODUCTION EDITOR
Robbie Kelly

SUBEDITOR
Caroline Fewkes

CHIEF EXECUTIVE OFFICER
Paul Howarth

Published in the United Kingdom
by Law Business Research Ltd, London
87 Lancaster Road, London, W11 1QQ, UK
© 2017 Law Business Research Ltd
www.TheLawReviews.co.uk

No photocopying: copyright licences do not apply.

The information provided in this publication is general and may not apply in a specific situation, nor does it necessarily represent the views of authors' firms or their clients. Legal advice should always be sought before taking any legal action based on the information provided. The publishers accept no responsibility for any acts or omissions contained herein. Although the information provided is accurate as of October 2017, be advised that this is a developing area.

Enquiries concerning reproduction should be sent to Law Business Research, at the address above.

Enquiries concerning editorial content should be directed
to the Publisher – gideon.roberton@lbresearch.com

ISBN 978-1-910813-89-8

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

THE LAW REVIEWS

THE MERGERS AND ACQUISITIONS REVIEW

THE RESTRUCTURING REVIEW

THE PRIVATE COMPETITION ENFORCEMENT REVIEW

THE DISPUTE RESOLUTION REVIEW

THE EMPLOYMENT LAW REVIEW

THE PUBLIC COMPETITION ENFORCEMENT REVIEW

THE BANKING REGULATION REVIEW

THE INTERNATIONAL ARBITRATION REVIEW

THE MERGER CONTROL REVIEW

THE TECHNOLOGY, MEDIA AND
TELECOMMUNICATIONS REVIEW

THE INWARD INVESTMENT AND
INTERNATIONAL TAXATION REVIEW

THE CORPORATE GOVERNANCE REVIEW

THE CORPORATE IMMIGRATION REVIEW

THE INTERNATIONAL INVESTIGATIONS REVIEW

THE PROJECTS AND CONSTRUCTION REVIEW

THE INTERNATIONAL CAPITAL MARKETS REVIEW

THE REAL ESTATE LAW REVIEW

THE PRIVATE EQUITY REVIEW

THE ENERGY REGULATION AND MARKETS REVIEW

THE INTELLECTUAL PROPERTY REVIEW

THE ASSET MANAGEMENT REVIEW

THE PRIVATE WEALTH AND PRIVATE CLIENT REVIEW

THE MINING LAW REVIEW

THE EXECUTIVE REMUNERATION REVIEW

THE ANTI-BRIBERY AND ANTI-CORRUPTION REVIEW

THE CARTELS AND LENIENCY REVIEW

THE TAX DISPUTES AND LITIGATION REVIEW

THE LIFE SCIENCES LAW REVIEW

THE INSURANCE AND REINSURANCE LAW REVIEW

THE GOVERNMENT PROCUREMENT REVIEW
THE DOMINANCE AND MONOPOLIES REVIEW
THE AVIATION LAW REVIEW
THE FOREIGN INVESTMENT REGULATION REVIEW
THE ASSET TRACING AND RECOVERY REVIEW
THE INSOLVENCY REVIEW
THE OIL AND GAS LAW REVIEW
THE FRANCHISE LAW REVIEW
THE PRODUCT REGULATION AND LIABILITY REVIEW
THE SHIPPING LAW REVIEW
THE ACQUISITION AND LEVERAGED FINANCE REVIEW
THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW
THE PUBLIC-PRIVATE PARTNERSHIP LAW REVIEW
THE TRANSPORT FINANCE LAW REVIEW
THE SECURITIES LITIGATION REVIEW
THE LENDING AND SECURED FINANCE REVIEW
THE INTERNATIONAL TRADE LAW REVIEW
THE SPORTS LAW REVIEW
THE INVESTMENT TREATY ARBITRATION REVIEW
THE GAMBLING LAW REVIEW
THE INTELLECTUAL PROPERTY AND ANTITRUST REVIEW
THE REAL ESTATE M&A AND PRIVATE EQUITY REVIEW
THE SHAREHOLDER RIGHTS AND ACTIVISM REVIEW
THE ISLAMIC FINANCE AND MARKETS LAW REVIEW
THE ENVIRONMENT AND CLIMATE CHANGE LAW REVIEW
THE CONSUMER FINANCE LAW REVIEW
THE INITIAL PUBLIC OFFERINGS REVIEW
THE CLASS ACTIONS LAW REVIEW
THE TRANSFER PRICING LAW REVIEW
THE BANKING LITIGATION LAW REVIEW
THE HEALTHCARE LAW REVIEW

www.TheLawReviews.co.uk

ACKNOWLEDGEMENTS

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

ALLENS

ASTREA

BAKER & MCKENZIE – CIS, LIMITED

BOGSCH & PARTNERS LAW FIRM

DUCLOS, THORNE, MOLLET-VIÉVILLE & ASSOCIÉS (DTMV)

JUN HE LLP

KOBYLAŃSKA & LEWOSZEWSKI KANCELARIA PRAWNA SP J

LEE & KO

M&M BOMCHIL

NNOVATION LLP

PERCHSTONE & GRAEYS

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SIQUEIRA CASTRO – ADVOGADOS

SK CHAMBERS

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

VDA VIEIRA DE ALMEIDA

WALDER WYSS LTD

WINHELLER RECHTSANWALTSGESELLSCHAFT MBH

CONTENTS

Chapter 1	GLOBAL OVERVIEW.....	1
	<i>Alan Charles Raul</i>	
Chapter 2	EUROPEAN UNION OVERVIEW.....	5
	<i>William RM Long, Géraldine Scali, Francesca Blythe and Alan Charles Raul</i>	
Chapter 3	APEC OVERVIEW.....	26
	<i>Ellyce R Cooper and Alan Charles Raul</i>	
Chapter 4	ARGENTINA.....	39
	<i>Adrián Lucio Furman, Francisco Zappa and Catalina Malara</i>	
Chapter 5	AUSTRALIA.....	49
	<i>Michael Morris</i>	
Chapter 6	BELGIUM.....	62
	<i>Steven De Schrijver</i>	
Chapter 7	BRAZIL.....	81
	<i>Daniel Pitanga Bastos de Souza and Bruno Granzotto Giusto</i>	
Chapter 8	CANADA.....	90
	<i>Shaun Brown</i>	
Chapter 9	CHINA.....	105
	<i>Marissa (Xiao) Dong</i>	
Chapter 10	FRANCE.....	117
	<i>Arnaud Vanbremeersch and Christophe Clarenc</i>	
Chapter 11	GERMANY.....	131
	<i>Nikola Werry, Benjamin Kirschbaum and Jens-Marwin Koch</i>	

Contents

Chapter 12	HONG KONG	144
	<i>Yuet Ming Tham</i>	
Chapter 13	HUNGARY.....	159
	<i>Tamás Gödölle</i>	
Chapter 14	INDIA	176
	<i>Aditi Subramaniam and Sanuj Das</i>	
Chapter 15	JAPAN	190
	<i>Tomoki Ishiara</i>	
Chapter 16	KOREA	206
	<i>Kwang Bae Park and Ju Bong Jang</i>	
Chapter 17	MALAYSIA	220
	<i>Shanthi Kandiah</i>	
Chapter 18	MEXICO	234
	<i>César G Cruz-Ayala and Diego Acosta-Chin</i>	
Chapter 19	NIGERIA.....	247
	<i>Folabi Kuti, Ugochukwu Obi and Seth Azubuike</i>	
Chapter 20	POLAND.....	260
	<i>Anna Kobylańska and Marcin Lewoszewski</i>	
Chapter 21	PORTUGAL.....	272
	<i>Magda Cocco and Inês Antas de Barros</i>	
Chapter 22	RUSSIA	284
	<i>Elena Kukushkina, Georgy Mzhavanadze and Vadim Perevalov</i>	
Chapter 23	SINGAPORE.....	296
	<i>Yuet Ming Tham</i>	
Chapter 24	SPAIN.....	314
	<i>Leticia López-Lapuente and Reyes Bermejo Bosch</i>	
Chapter 25	SWITZERLAND	327
	<i>Jürg Schneider, Monique Sturny and Hugh Reeves</i>	

Contents

Chapter 26	UNITED KINGDOM.....	347
	<i>William RM Long, Géraldine Scali and Francesca Blythe</i>	
Chapter 27	UNITED STATES.....	364
	<i>Alan Charles Raul, Frances E Faircloth and Vivek K Mohan</i>	
Appendix 1	ABOUT THE AUTHORS.....	393
Appendix 2	CONTRIBUTING LAW FIRMS' CONTACT DETAILS.....	409

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 the European Union (EU) principles² 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 EU Data Protection Directive 95/46/EC.

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 Commissioner has issued a Public Consultation Paper⁴ entitled Personal Data Protection (Transfer Of Personal Data To Places Outside Malaysia) Order 2017 (the Proposed Order 2017), marking an important milestone in the personal data export restriction found in Section 129(1) of the PDPA. The Proposed Order 2017 seeks feedback from the public on the Commissioner's draft whitelist of countries to which personal data originating in Malaysia may be freely transferred without having to rely on exemptions provided by Section 129(3) of the PDPA.⁵

The Commissioner has also moved towards the enforcement phase of PDPA implementation. In early May 2017, a company in the education industry was charged under the PDPA for processing the personal data of former employees without a certificate of registration.⁶

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;

4 (PCP) No. 1/2017.

5 See Section IX.

6 See Section VII.ii.

- 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.

Complaints remain the primary trigger for the investigation and enforcement activities of the Commissioner. As of April 2017, the Commissioner has received over 330 official complaints since the coming into force of the law. Unsurprisingly, approximately 85 per cent of complaints relate to processing of data in the electronic environment.⁷

Cybersecurity issues have also received significant media attention as Malaysian companies were not spared in the global ransomware attacks, such as the WannaCry cyberattack. On 9 June 2017, the deputy prime minister of Malaysia, Datuk Seri Dr Ahmad Zahid Hamidi, announced that the Malaysian government will introduce a new law that is aimed at protecting Malaysians from cybersecurity threats in light of the fact that there are about 10,000 cybersecurity-related reports received every year by the government. Malaysia does not have a specific law addressing cybersecurity-related offences. Enforcement agencies, such as the National Cyber Security 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. It is expected that the NCSA would be placed under the umbrella of the National Security Council⁸ and will function as the agency that coordinates all efforts to manage cyberthreats.

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.⁹ 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

7 Conference on the PDPA organised by the Personal Data Protection Department at Hotel Istana, Kuala Lumpur on 23 May 2017.

8 The National Security Council is a federal agency under the Prime Minister’s Department and is responsible for managing and coordinating the implementation of policies related to the security of Malaysia.

9 Section 5(2) of the PDPA.

for the Utilities Sector (Electricity),¹⁰ the Personal Data Protection Code of Practice for the Insurance/Takaful Industry¹¹ and the Personal Data Protection Code of Practice for the Banking and Financial Sector.¹²

Non-compliance with the codes will also carry penal consequences.¹³

Personal data

Three conditions must be fulfilled for any data to be considered as 'personal data' within the ambit of the PDPA.¹⁴

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.¹⁵ 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.¹⁶

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.¹⁷

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.¹⁸

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.

10 With effect from 23 June 2016.

11 With effect from 23 December 2016.

12 With effect from 19 January 2017.

13 Section 29 of the PDPA.

14 Section 2 of the PDPA.

15 Section 2 of the PDPA.

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

17 Section 2 of the PDPA.

18 Section 40(1) of the PDPA.

'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.

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 has been expanded in 2016 to include two additional sectors: pawnbroking and money lending.¹⁹

Failure to register by these categories of data users is an offence.²⁰

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.²¹

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

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

20 Section 16(4) of the PDPA.

21 Section 6(2) of the PDPA.

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.²²

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

22 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.

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;²³
- b* the right to correct personal data;²⁴
- c* the right to withdraw consent;²⁵
- d* the right to prevent processing likely to cause damage or distress;²⁶ and
- e* the right to prevent processing for purposes of direct marketing.²⁷

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.

23 Section 30 of the PDPA.

24 Section 34 of the PDPA.

25 Section 38 of the PDPA.

26 Section 42 of the PDPA.

27 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.²⁸ 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.²⁹

The Guidelines on Data Management and MIS³⁰ 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.³¹

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

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 Communication and Multimedia Malaysia and this is then published in the Gazette. The places identified in the Proposed Order 2017³² are as follows: European Economic Area member countries, the United Kingdom, the

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

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

30 Management Information System.

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

32 See Section II.

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.

Until the Proposed Order 2017 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 spelled out in specific terms as yet; however, these are likely to be specifically provided for in the near future. A 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 ensuring 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.³³ 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.

33 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.³⁴

ii Recent enforcement cases

In May 2017, a company operating a private college was charged with processing personal data without a certificate of registration under Section 16(4) of the PDPA. This offence carries a maximum fine of 500,000 ringgit or up to three years in jail, or both. This action is the very first case in Malaysia involving a breach of the PDPA. The office of the Commissioner has said that there are other cases in the pipeline.

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.

³⁴ Section 133(1) of the PDPA.

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 2016 – MyCERT Incident Statistics – indicate that in 2016 alone there were over 8,000 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 Cyber Security 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.

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

- a* assess the implementation of multilayered 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 cyber threats, uncover new cyber-attack 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 Cyber laws

In contrast to the comprehensive approach of the PDPA, Malaysia's cyber laws are scattered across various pieces of legislation, although this will be more streamlined when the proposed new cybersecurity law (which seeks to empower the NCSA to coordinate responses to cyberthreats) comes into effect. Presently, the key provisions of Malaysia's cyber laws are as follows.

35 www.mycert.org.my/statistics/2016.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 cyber offences include:

- a* cyber pornography and exploitation of children;⁴²
- b* online sedition and internet defamation;⁴³
- c* misuse of computers;⁴⁴
- d* prostitution and other illegal cyber sexual activities; and
- e* cyber terrorism.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 require any person operating a cyber cafe and cyber centre 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 cyber terrorism, 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. In terms of inspection visits, the Commissioner's focus appears to be set on sectors processing large quantities of personal data.

Compliance with the General Data Protection Directive (GDPR) 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 looming implementation deadline of 25 May 2018. The GDPR's prescriptions on organisational and technical measures to protect personal data are likely to influence Malaysian standard setting as well.

An area that would benefit from more explicit standard setting, given the ubiquitous reliance on the internet for commercial transactions, relates to the technological measures for protecting personal or sensitive personal data, such as data classification, data loss prevention, encryption, managing consent and data transfer limitations, as standards vary significantly in Malaysian corporations.

The installation of a centralised agency to enforce cybersecurity breaches in the country is a game changer. The precise jurisdictional scope and extent of powers given to this agency, however, remains unclear.

ABOUT THE AUTHORS

SK CHAMBERS

9B Jalan Setiapuspa
Bukit Damansara
50490 Kuala Lumpur
Malaysia
Tel: +603 2011 6800
Fax: +603 2011 6801
sk@skchambers.co
www.skchambers.co

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 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.

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



Strategic Research Sponsor of the
ABA Section of International Law



ISBN 978-1-910813-89-8