# The Privacy, Data Protection and Cybersecurity Law Review

Third Edition

Editor
Alan Charles Raul

Law Business Research

# The Privacy, Data Protection and Cybersecurity Law Review

Third Edition

Editor
Alan Charles Raul

Law Business Research Ltd

PUBLISHER
Gideon Roberton

SENIOR BUSINESS DEVELOPMENT MANAGER
Nick Barette

BUSINESS DEVELOPMENT MANAGER
Thomas Lee

SENIOR ACCOUNT MANAGERS
Felicity Bown, Joel Woods

ACCOUNT MANAGERS
Jessica Parsons, Jesse Rae Farragher

MARKETING COORDINATOR
Rebecca Mogridge

EDITORIAL ASSISTANT
Gavin Jordan

HEAD OF PRODUCTION
Adam Myers

PRODUCTION EDITOR
Anne Borthwick

SUBEDITOR
Anna Andreoli

CHIEF EXECUTIVE OFFICER
Paul Howarth

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

www.TheLawReviews.co.uk


ISBN 978-1-910813-32-4

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

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

CMS CAMERON MCKENNA GRESZTA I SAWICKI SP.K

DUNAUD CLARENC COMBLES & ASSOCIÉS

ELIG, ATTORNEYS-AT-LAW

GIANNI, ORIGONI, GRIPPO, CAPPELLI & PARTNERS

JUN HE LAW OFFICES

LEE & KO

MATHESON

NNOVATION LLP

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SIQUEIRA CASTRO – ADVOGADOS

SK CHAMBERS

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

VIEIRA DE ALMEIDA & ASSOCIADOS, SP RL

WALDER WYSS LTD

WINHELLER RECHTSANWALTSGESELLSCHAFT MBH

# CONTENTS

# Chapter 18

# 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 facilitate electronic commerce and business transactions,[2] hence its application only to commercial transactions. It was seen as necessary step to combat credit card fraud, identity theft and selling of personal data without customer consent, and to build consumer confidence. Before the PDPA, data protection obligations were spread out among certain sectoral secrecy and confidentiality obligations, while personal information was only 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'. The PDPA is enforced by the Commissioner of the Department of Personal Data Protection (Commissioner). It is based on a set of data protection principles akin to the European Union principles[3] 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.[4]

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

1 Shanthi Kandiah is a partner at SK Chambers.

2 Dato Seri Utama Dr Rais Yatim, Minister of Information, Communications and Culture Malaysia during the second and third reading of the Personal Data Protection Bill 2009, 12th Parliament, Third quarter, 5 April 2010.

3 EU Data Protection Directive 95/46/EC.

4 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

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.

### 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 they process. 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, *infra*).

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, *infra*. 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

By way of background, Phase 1 of the implementation programme for the PDPA saw the first set of subsidiary and supplemental legislation being released, namely the Class Data Users Order 2013 and the Registration of Data User Regulation 2013 requiring the registration of select categories of data users.[5]

The Commissioner has now embarked on Phase 2 of the implementation programme, which entails advisory and compliance visits by the Personal Data Protection Department's enforcement teams. The second phase will also see more guidelines and codes of practice being issued.

As at August 2015, the Commissioner had received 82 official complaints[6] (out of over 140 complaints). The Commissioner has stated that it is monitoring the trend in

enactments to perform specific public functions, such as Bank Negara Malaysia (BNM), the Employees Provident Fund, the Securities Commission and the Companies Commission of Malaysia, fall within the scope of this exemption.

5 Interpretive guidelines were also issued during this period, namely the Personal Data Protection Regulations published on 14 November 2013.

6 Complaints received through its Complaints Unit.

complaints to determine its policies going forward. On the whole, the Commissioner finds compliance to be low, but has found companies that are ISMS-compliant to have achieved a good measure of compliance.[7]

After several rounds of consultation with the public, the Commissioner issued the Personal Data Protection Standards 2015 on 23 December 2015 (Standards). The Standards (which carry criminal sanctions if not implemented) are considered the 'minimum' standards to be observed by companies in their handling of personal data of customers and employees.

On 23 June 2016, the first industrial code of practice was registered by the Commission covering the utility sector (electricity). An industrial code of practice is a set of industrial standards of conduct prepared by a data user form (a body designated by the Commissioner to represent a class of data users) to govern compliance with the PDPA. The codes take effect upon registration with the Commissioner, and non-compliance carries penal consequences.[8] Other codes of practice that are reported to be in the final stages of gaining the approval of the Commissioner are the codes of practice for the accounting and audit sectors, direct selling, insurance, banking and finance, engineering services and architecture.

In Phase 3, organisations should prepare for audit visits by the Commissioner and expect full enforcement of the PDPA, namely prosecution for non-compliance. As a precursor to full enforcement, the Compounding of Offences Regulation was issued on 14 March 2016. The Regulation specifies the offences that can be compounded under Section 132 of the PDPA, and provides details on how the offer, acceptance and payment of compoundable offences should be carried out.

## 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 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. As previously mentioned, the first industrial code of practice to come into force covers the utility sector (electricity). Non-compliance with the codes will also carry penal consequences.[10]

#### *Personal data*

Three conditions must be fulfilled for any data to be considered as 'personal data' within the ambit of the PDPA.[11]

7 Slide presentation from the website of the Personal Data Protection Department.

8 Section 29 of the PDPA.

9 Section 5(2) of the PDPA.

10 Section 29 of the PDPA.

11 Section 2 of the PDPA.

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.[12] There is some ambiguity as to whether an activity must have a profit motivation to be considered a commercial transaction.

Second, such 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.[13]

***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.[14]

Sensitive personal data may only be processed with the explicit consent of the data subject, if the sensitive personal data has been made public by the data subject or if the processing satisfies certain statutory conditions set out in the PDPA.[15]

***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 of such 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 authorizes 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 will not be bound directly by the provisions of the PDPA.

12 Section 2 of the PDPA.

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

14 Section 2 of the PDPA.

15 Section 40(1) of the PDPA.

### ii General obligations for data handlers

***Registration***

The Class 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.

Failure by these categories of data users to register is an offence.[16]

***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.[17]

***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 provide that the data user must keep a record of consents from data subjects. The Regulations further provide that the Commissioner or an inspection officer may require production of the record of consents. It places the burden of proof for consent squarely on the data user.

Helpfully, the code of practice for the utility sector (electricity) provides examples of consent, whether express or implied, that must be recorded or maintained by the data user.

Examples of such methods 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.

16 Section 16(4) of the PDPA.
17 Section 6(2) of the PDPA.

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

***Explicit consent***

Regarding explicit consent, the code of practice for the utility 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 statement 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 such 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 to the data user.[18]

***Retention***

Personal data should not be kept longer than necessary. 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 such 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;[19]
*b* the right to correct personal data;[20]
*c* the right to withdraw consent;[21]
*d* the right to prevent processing likely to cause damage or distress;[22] and
*e* the right to prevent processing for purposes of direct marketing.[23]

18 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.
19 Section 30 of the PDPA.
20 Section 34 of the PDPA.
21 Section 38 of the PDPA.
22 Section 42 of the PDPA.
23 Section 43 of the PDPA.

### 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 (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 telecommunication 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.

#### *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.[24] 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.[25]

The Guidelines on Data Management and the management information system (MIS) 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

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

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

in scope to the seven PDPA principles) for the telecommunications and multimedia sectors. The GCC binds all licensed service providers under the Communications and Multimedia Act 1998 (CMA) and all non-licensed service providers who are members of the Consumer Forum.[26]

*Direct marketing*

The PDPA prescribes direct selling and direct marketing 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 marketer or direct seller stop or even 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 list has not been prescribed as yet. Exemptions from this requirement include where the transfer was consented to by the data subject; or 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 that place of transfer in any manner that, if that place is Malaysia, would be a contravention of the PDPA.[27] 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 such 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.

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

27 See Section V.iv, *infra*.

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 Personal Data Protection Standards 2015 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 Personal Data Protection Regulations 2013 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.[28] Some of the more 'challenging' standards for implementation are the standards that stipulate that the transfer of personal data through removable media devices (e.g., USB thumb-drives) and cloud computing services (e.g., Dropbox, 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 removable media device must be recorded. Additionally, data users are required to record access to personal data, and to make available such records to the Commissioner upon request.

**vi Incident response plan**

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

28 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; or where the disclosure is necessary for the purpose of preventing or detecting a crime, or for the purpose of investigations.[29]

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.

## 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 such 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 such authorised public officer reasonably believes has committed or is attempting to commit an offence under the PDPA.

29 Section 39(b)(i) of the PDPA. This information is also exempted from the general principle, notice and choice principle, access principle and other related provisions of the Act.

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, director, chief executive officer, chief operating officer, manager, secretary or other similar officer, such entity or person may be deemed to have committed the offence unless it, he or she can establish 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.[30]

### ii Recent enforcement cases

While there is no official report on any enforcement actions, it should be noted that the Commissioner has carried out onsite monitoring activities on data users since early 2015.

### 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 such individual's personal data.

## 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 of Malaysia, unless such data is intended to be further processed in Malaysia.

## IX CYBERSECURITY AND DATA BREACHES

Statistics from Cybersecurity Malaysia for 2015 – MyCERT Incident Statistics – indicate that in 2015 alone there were 9,915 reports on cyber-related incidents.[31] 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 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. Being ISMS-certified was seen as a strategy to promote the trust of foreign companies and potential trading partners in the ability of their Malaysian counterparts to safeguard their data and information.

30 Section 133(1) of the PDPA.

31 www.mycert.org.my/statistics/2015.php.

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 multi-layered security architecture;
*b* ensure security controls for server-to-server external network connections;
*c* ensure the effectiveness of the monitoring undertaken by Security Operation Center 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 also issued a public consultation paper on 21 March 2016 on the proposed regulatory framework on cybersecurity resilience for capital market participants' management of cybersecurity risks.[32]

**i Cyber laws**

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

*CMA*

*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;[33]
*b* the offence of using an apparatus or device without authority;[34]
*c* the offence of improper use of network facilities or network services – such annoying, abusive, threatening, harassing or obscene communications – e-mails (spamming), SMS, MMS website content publishing;[35]
*d* the offence of interception and disclosure of communications;[36] and
*e* the offence of damage to network facilities.[37]

Other cyber offences include:

*a* cyber pornography and exploitation of children;[38]
*b* online sedition and internet defamation;[39]

32 Securities Commission Public Consultation Paper No. 1/2016 Proposed Regulatory Framework on Cybersecurity Resilience, 21 March 2016.
33 Section 233(1)(a) of the CMA.
34 Section 231 of the CMA.
35 Section 233 of the CMA.
36 Section 234 of the CMA.
37 Section 235 of the CMA.
38 Section 292, 293 and 294 of the Penal Code, Section 5 of Film Censorship Act 2002 and Section 31 Child Act 2001.
39 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.

*c* misuse of computers;[40]
*d* prostitution and other illegal cyber sexual activities; and
*e* cyber terrorism.[41]

### 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 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 regulations, guidelines and codes of practice being issued over the course of the year. This will provide greater clarity regarding the Commissioner's expectations.

It is further anticipated that the government will continue to exert greater control over internet content and transactions. The challenge will be to get the right balance so that the development of electronic commerce and online transactions is not inhibited.

40 Section 3 (unauthorised access to computer materials), Section 4 (unauthorized 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.

41 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).

## Appendix 1

# ABOUT THE AUTHORS

**SHANTHI KANDIAH**

*SK Chambers*

Shanthi Kandiah founded SK Chambers with the goal of creating a standalone 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, 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.

**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