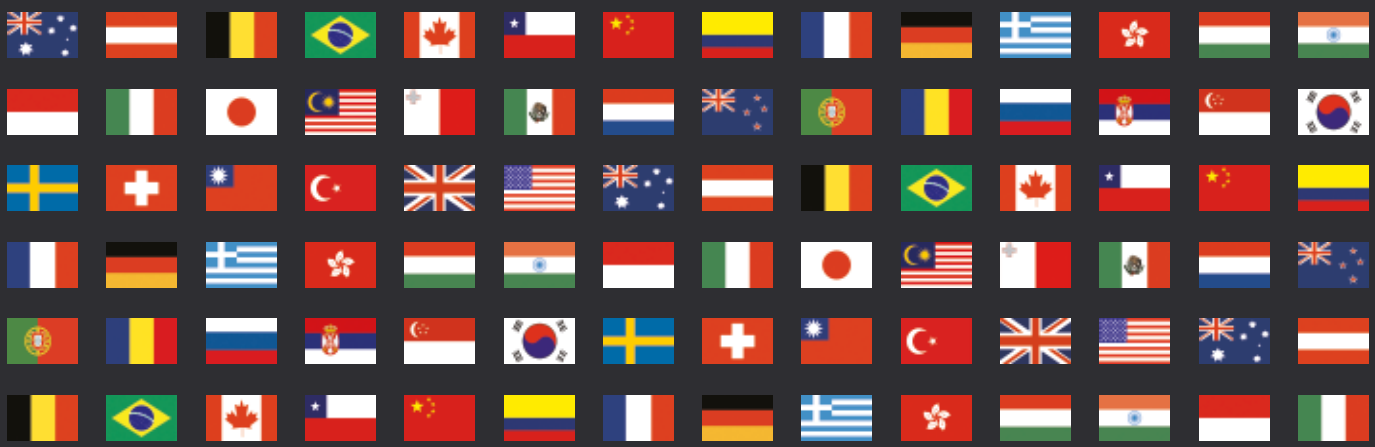
Data Protection & Privacy 2021

Contributing editors
Aaron P Simpson and Lisa J Sotto



LEXOLOGY
Getting The Deal Through

Publisher
Tom Barnes
tom.barnes@lbresearch.com

Subscriptions
Claire Bagnall
claire.bagnall@lbresearch.com

Senior business development manager
Adam Sargent
adam.sargent@gettingthedealthrough.com

Published by
Law Business Research Ltd
Meridian House, 34-35 Farringdon Street
London, EC4A 4HL, UK

First published 2012
Ninth edition
ISBN 978-1-83862-322-7

Printed and distributed by
Encompass Print Solutions
Tel: 0844 2480 112

Data Protection & Privacy

2021

Contributing editors
Aaron P Simpson and Lisa J Sotto
Hunton Andrews Kurth LLP

Lexology Getting The Deal Through is delighted to publish the ninth edition of *Data Protection & Privacy*, which is available in print and online at www.lexology.com/gtdt.

Lexology Getting The Deal Through provides international expert analysis in key areas of law, practice and regulation for corporate counsel, cross-border legal practitioners, and company directors and officers.

Throughout this edition, and following the unique Lexology Getting The Deal Through format, the same key questions are answered by leading practitioners in each of the jurisdictions featured. Our coverage this year includes new chapters on Canada and Romania.

Lexology Getting The Deal Through titles are published annually in print. Please ensure you are referring to the latest edition or to the online version at www.lexology.com/gtdt.

Every effort has been made to cover all matters of concern to readers. However, specific legal advice should always be sought from experienced local advisers.

Lexology Getting The Deal Through gratefully acknowledges the efforts of all the contributors to this volume, who were chosen for their recognised expertise. We also extend special thanks to the contributing editors, Aaron P Simpson and Lisa J Sotto of Hunton Andrews Kurth LLP, for their continued assistance with this volume.

LEXOLOGY®
Getting The Deal Through

London
August 2020

Reproduced with permission from Law Business Research Ltd
This article was first published in September 2020
For further information please contact editorial@gettingthedealthrough.com

Contents

Malaysia

Jillian Chia Yan Ping and Natalie Lim
SKRINE

LAW AND THE REGULATORY AUTHORITY

Legislative framework

1 Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments on privacy or data protection?

The Personal Data Protection Act 2010 (PDPA), which is based on data protection principles akin to those found in the EU Data Protection Directive 95/46/EC (the General Data Protection Regulation (GDPR)), came into force on 15 November 2013. The following subsidiary legislations have since been enacted under the PDPA:

1 Personal Data Protection Regulations 2013;
2 Personal Data Protection (Class of Data Users) Order 2013;
3 Personal Data Protection (Registration of Data User) Regulations 2013;
4 Personal Data Protection (Fees) Regulations 2013; and
5 Personal Data Protection (Compounding of Offence) Regulations 2016.

The Personal Data Protection Standard 2015 (PDP Standard) also sets out the minimum standards to be observed by data users when handling personal data and the following enforceable codes of practice have been registered:

1 Utilities Sector (Electricity);
2 Insurance/Takaful Industry;
3 Banking and Financial Sector;
4 Transportation Sector (Aviation); and
5 Communications Sector.

Data protection authority

2 Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

As the responsible authority in Malaysia, the functions of the Personal Data Protection Commissioner (Commissioner) include advising the Minister of Communications and Multimedia on the national data protection policy and implementing and enforcing data protection laws.

The Commissioner has the power to do all things necessary or expedient for or in connection with the performance of his functions under the PDPA. This includes the power to investigate (such as where the Commissioner has reasonable grounds to believe that the PDPA has been breached or is being breached or where a proper complaint has been lodged), inspect a data user's personal data system, access computerised data, and search and seize with or without warrant.

The Commissioner may also serve an enforcement notice upon investigation, which specifies the breach, remedial steps required and the deadline for compliance or, if necessary, direct the data user to cease processing.

Cooperation with other data protection authorities

3 Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

The PDPA does provide that it is a function of the Commissioner to liaise and cooperate with persons performing similar personal data protection functions in any place outside Malaysia in respect of matters of mutual interest, including matters concerning the privacy of individuals in relation to their personal data.

Breaches of data protection

4 Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Breaches of data protection law can lead to administrative sanctions and criminal penalties.

Depending on the nature of the offence, contravening the PDPA may lead to a fine between 100,000 ringgit and 500,000 ringgit and imprisonment of one to three years, although certain offences are compoundable, which may allow reduced penalties.

A breach of the PDPA may result in an inquiry or investigation by the Commissioner (either on its own initiative or based on a complaint received). Where following the investigation, the Commissioner decides that the PDPA has been contravened, the Commissioner may serve an enforcement notice, specifying the breach, the steps required to be taken to remedy the breach within a certain period and directing, if necessary, the relevant data user to cease processing the personal data. Fines of up to 200,000 ringgit or two years' imprisonment or both are possible for failure to comply with the Commissioner's enforcement notice.

Generally, a breach of any of the seven data protection principles may incur a fine of up to 300,000 ringgit and two years' imprisonment.

The Commissioner may also revoke the registration of a data user in certain circumstances, (eg, if the data user has failed to comply with the provisions of the PDPA or with any conditions imposed as part of the registration).

If a business commits an offence, its directors, chief executive officers, chief operating officers and other similar officers may be charged severally or jointly for non-compliance by the business, subject to certain limited defences.

SCOPE

Exempt sectors and institutions

5 Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

The Personal Data Protection Act 2010 (PDPA) governs personally identifiable data which is processed in respect of a 'commercial transaction' but certain sectors and types of processing are exempted, such as:

- Processing of information for the purpose of a credit reporting business carried on by a credit reporting agency under the Credit Reporting Agencies Act 2010; and
- Processing of information by the Malaysian federal and state governments.

Communications, marketing and surveillance laws

6 Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

There are no express provisions on interception of communications or monitoring and surveillance of individuals under the PDPA but to the extent that it involves processing of personal data in respect of commercial transactions, the PDPA would apply. Electronic marketing is also subject to the PDPA and on marketing, the PDPA does give the individual the right to require a data user to cease or not to begin processing his personal data for the purposes of 'direct marketing' (communication by any means which is directed to particular individuals).

The telecommunications and computer crimes laws also generally prohibit unlawful interception of communications or unauthorised access or use or interception of any computer or device. Electronic marketing must also not be done in a way that may contravene our telecommunications law which prohibit communications initiated with the intention to annoy, abuse, threaten or harass a person.

Other laws

7 Identify any further laws or regulations that provide specific data protection rules for related areas.

Various laws apply depending on the specific type of data. Below are just some examples of laws which apply to financial and health data.

The Financial Services Act 2013 (FSA) prohibits disclosure of any document/information relating to the affairs or account of a customer of a financial institution to another person except in certain permitted circumstances. The Central Bank of Malaysia has also issued the Guidelines on Data Management and MIS Framework (BNM Guidelines) to govern the data management by the financial sector. The BNM Guidelines is applicable to all the institutions licensed under the FSA and all the institutions licensed under the Islamic Financial Services Act 2013.

The Private Healthcare Facilities and Services (Private Medical Clinics or Private Dental Clinics) Regulations 2006 also govern the processing, management and retention of patients' medical records and the processing of healthcare information is also governed by certain confidentiality guidelines issued by the Malaysian Medical Council.

PII formats

8 What forms of PII are covered by the law?

Any information relating directly or indirectly to an individual who is identified or identifiable from that information or from that and other information in the data user's possession is considered personal data within the ambit of the PDPA. Such broad definition includes data in electronic and manual form.

Extraterritoriality

9 Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

The PDPA applies to data users who are:

- established in Malaysia (and the personal data is processed by that person or any other person employed or engaged by that establishment); or
- not established in Malaysia, but use equipment in Malaysia to process the personal data otherwise than for the purposes of transit through Malaysia.

The PDPA will not apply to any personal data processed outside Malaysia, unless it is intended to be further processed in Malaysia.

Covered uses of PII

10 Is all processing or use of PII covered? Is a distinction made between those who control or own PII and those who provide PII processing services to owners? Do owners', controllers' and processors' duties differ?

'Processing' is defined widely to include collection, recording, storage and use of personal data, but the PDPA applies to personal data processed in respect of a commercial transaction only. Certain types of processing are also exempted (eg, processing by an individual only for his or her personal, family or household affairs is exempted).

The PDPA distinguishes between a 'data user', 'data processor' and 'data subject'. A data user, which is conceptually similar to a controller, 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 processor. A data processor means any person other than an employee of the data user who processes personal data solely on behalf of the data user, and does not process the personal data for any of his own purposes. The obligations are imposed on the data user and there are specific obligations imposed on the data user where a data processor is used. However, the data processor is not bound directly under the PDPA.

LEGITIMATE PROCESSING OF PII

Legitimate processing – grounds

11 Does the law require that the holding of PII be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

The Personal Data Protection Act 2010 (PDPA) requires consent (for processing of non-sensitive personal data) and explicit consent (for processing of sensitive personal data), failing which the processing must be legitimised on specific grounds for exemptions. For non-sensitive personal data, the PDPA provides certain exemptions where the processing is necessary:

- for the performance of a contract to which the individual is a party;
- for the taking of steps at the request of the individual with a view to entering into a contract;
- for compliance with any legal obligation to which the data user is the subject, other than an obligation imposed by a contract;
- to protect the individual's vital interests;
- for the administration of justice; or
- for the exercise of any functions conferred on any person by or under any law.

Processing sensitive personal data without explicit consent is subject to separate exemptions.

But there are conditions for processing which the data user must comply with (regardless of whether consent or explicit consent has been obtained). Personal data shall not be processed unless:

- the personal data is processed for a lawful purpose directly related to an activity of the data user;
- the processing of the personal data is necessary for or directly related to that purpose;
- the personal data is adequate but not excessive in relation to that purpose;
- the processing of the personal data is necessary for or directly related to that purpose; and
- the personal data is adequate but not excessive in relation to that purpose.

Legitimate processing – types of PII

12 | Does the law impose more stringent rules for specific types of PII?

Stricter rules apply to processing of 'sensitive personal data', which includes information relating to mental or physical health, political opinions, religious beliefs and other beliefs of a similar kind as well as information relating to the commission or alleged commission of any offence or any other personal data as the minister may determine by a gazette order. Processing sensitive personal data requires explicit consent unless an exemption applies. Some examples are where the processing relates to information that has been made public as a result of steps deliberately taken by the data subject or where the processing is necessary:

- for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data user in connection with employment;
- to protect the vital interests of the data subject or another person, where consent cannot be given by or on behalf of the data subject or the data user cannot reasonably be expected to obtain the consent of the data subject;
- to protect the vital interests of another person, where consent by or on behalf of the data subject has been unreasonably withheld; or
- for the purposes of obtaining legal advice, or the establishment, exercising or defence of legal claims.

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PII

Notification

13 | Does the law require owners of PII to notify individuals whose PII they hold? What must the notice contain and when must it be provided?

A data user must notify the individual in writing in English and Malay of the following:

- that the individual's personal data is being processed by or on behalf of the data user, with a description of the personal data;
- the purposes for which the personal data is being or is to be collected and further processed;
- of any information available to the data user as to the source of that personal data;
- of the individual's right to request access to and to request correction of the personal data and how to contact the data user with any inquiries or complaints in respect of the personal data;
- of the class of third parties to whom the data user discloses or may disclose the personal data;
- of the choices and means the data user offers the individual for limiting the processing of personal data, including personal data relating to other persons who may be identified from that personal data;
- whether it is obligatory or voluntary for the individual to supply the personal data; and
- where obligatory, the consequences of failure to supply the personal data.

The notice must also be given 'as soon as practicable' either when:

- the individual is first asked by the data user to provide his personal data;
- when the data user first collects the personal data; or
- in any other case before the data user uses the personal data for a purpose other than the purpose for which the personal data was collected or before the data user discloses the personal data to a third party.

Exemption from notification

14 | When is notice not required?

Notice is not required when personal data:

- is processed for the prevention or detection of crime or for the purpose of investigations, apprehension or prosecution of offenders, or assessment or collection of any tax or duty or other similar impositions;
- is processed for the purposes of preparing statistics or carrying out research provided that the resulting statistics or research results are not in a form which identifies the individual;
- is necessary for or in connection with any court judgment or order;
- is processed to discharge regulatory functions if the application of those provisions to the personal data would be likely to prejudice the proper discharge of those functions; and
- is processed for journalistic, literary or artistic purposes, provided that the processing is undertaken with a view to the publication by any person of the journalistic, literary or artistic material, the publication would be in the public interest and compliance with the provision in respect of which the exemption is claimed is incompatible with the journalistic, literary or artistic purposes.

Control of use

15 | Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

The data user must notify the individual of the choices and means for limiting the processing of personal data, including personal data relating to other persons who may be identified from that personal data.

The Personal Data Protection Act 2010 (PDPA) also gives the individual the right to withdraw consent and certain qualified rights (eg, the right to access and correct personal data, prevent processing likely to cause damage and distress and prevent processing for direct marketing).

Data accuracy

16 | Does the law impose standards in relation to the quality, currency and accuracy of PII?

Data users must take reasonable steps to ensure the personal data is accurate, complete, not misleading and kept up to date, having regard to the purpose (and any directly related purpose) for which it was collected and processed. Data users must also comply with the data integrity standards set by the Personal Data Protection Commissioner (Commissioner) (eg, the data user must update the personal data

immediately upon receiving a data correction notice from the individual and notify the individual of the update through appropriate methods).

Amount and duration of data holding

17 Does the law restrict the amount of PII that may be held or the length of time it may be held?

Personal data cannot be kept longer than is necessary to fulfil the processing purpose unless a longer retention period is required by law (eg, our tax laws generally require all relevant records and documents to be retained for seven years). Retention must be in accordance with the retention standards set by the Commissioner, which further specify the timeframe (eg, the data user must dispose of any personal data collection forms used for commercial transactions within 14 days, unless they carry legal value in relation with the commercial transaction).

Finality principle

18 Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

The 'finality principle' is not expressly featured in the PDPA but there are similar conditions of processing under the General Principle, where data users may not process personal data unless it is for a lawful purpose directly related to the data user's activity, the processing is necessary and directly related to the purpose, and the personal data are adequate and not excessive in relation to that purpose. Processing must also be restricted to the purposes described in the notice.

Use for new purposes

19 If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

For new purposes, consent must be obtained again unless any of the exceptions to the consent (or explicit consent) requirement applies. The notice must also be amended to cater for the new purpose.

SECURITY

Security obligations

20 What security obligations are imposed on PII owners and service providers that process PII on their behalf?

Data users must take practical steps to protect personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction by having regard:

- to the nature of the personal data and the harm that would result from such loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction;
- to the place or location where the personal data is stored;
- to any security measures incorporated into any equipment in which the personal data is stored;
- to the measures taken for ensuring the reliability, integrity and competence of personnel having access to the personal data; and
- to the measures taken for ensuring the secure transfer of the personal data.

If the processing is carried out by a data processor on behalf of a data user, the data user must ensure that the data processor:

- provides sufficient guarantees in respect of the technical and organisational security measures governing the processing; and
- takes reasonable steps to ensure compliance with those measures.

The data user must develop and implement a security policy that must be compliant with the Personal Data Protection Act 2010 (PDPA) and the security standards set by the Commissioner. The following is a brief uncomprehensive overview of the prescribed security standards:

- To ensure personnel who manage personal data are registered under a registration system before being granted access to personal data and to provide a user ID and password to staff given access to the personal data.
- To control and limit the authority of staff to access personal data for purposes of collection, processing and retention of the personal data.
- To ensure all staff involved in the processing of personal data always protects the confidentiality of personal data.
- To implement physical security procedures such as entry and exit controls, storage of personal data in locations which are safe from physical or natural threats and not exposed, installation of close circuit television around data storage areas (if required), and 24-hour security of facilities (if required).
- To implement back up and recovery systems.
- The latest antivirus software must be deployed and scheduled malware monitoring and scanning of operating systems to prevent attacks on electronically stored data must be implemented.
- To maintain proper access records to personal data periodically, which must be presented when instructed by the Commissioner.

In respect of non-electronically processed personal data:

- To prescribe physical security procedures such as:
  - to keep all personal data properly in a file;
  - keep all files containing personal data in a locked area;
  - keep all relevant keys in a safe place;
  - keep a record of key storage; and
  - to store personal data in an appropriate location.
- The transfer of personal data using conventional methods such as through post, by hand, fax or others must be recorded.
- To ensure that all used paper, printed documents or other documents which clearly shows personal data must be properly destroyed.
- Conduct awareness programmes on the responsibility to protect personal data for all relevant personnel (if necessary).

Notification of data breach

21 Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

The PDPA does not currently provide for this but the authorities issued a public consultation paper entitled 'The Implementation of Data Breach Notification', which seeks to introduce a data breach notification regime, where data users will be required to notify regulators and affected individuals in the event of a data breach. The consultation paper sets out, among others, the requirement to notify the Commissioner within 72 hours of becoming aware of the data breach incident and to provide details about the data at risk, actions that have been taken or will be taken to mitigate the risks to the data, details of notifications to affected individuals and details of the organisation's training programs on data protection. However, the consultation paper has yet to be gazetted as law.

INTERNAL CONTROLS

Data protection officer

22 | Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

The Personal Data Protection Act 2010 (PDPA) does not mandate the appointment of a data protection officer (DPO) but the application form for registration of data users requires a 'compliance person' to be named which is indicated as the individual who will 'supervise the application of the PDPA' in the data user's organisation. A proposal paper entitled 'Guidelines on Compliance with Personal Data Protection 2010' seeking to introduce the designation of such officer was issued in 2014 but until it is gazetted as law, its status remains unclear.

Record keeping

23 | Are owners or processors of PII required to maintain any internal records or establish internal processes or documentation?

A data user must keep and maintain a record of any application, notice, request or any other information relating to personal data processed by him in the form and manner that may be determined by the Personal Data Protection Commissioner (Commissioner).

The personal data system must also be open for inspection and the Commissioner or inspection officer may require certain documents to be produced including records of consent and notices, list of disclosures to third parties and the security policies. Other laws may also prescribe record-keeping requirements (eg, tax laws).

New processing regulations

24 | Are there any obligations in relation to new processing operations?

The PDPA does not presently require data users to apply a privacy-by-design approach or carry out privacy impact assessments.

REGISTRATION AND NOTIFICATION

Registration

25 | Are PII owners or processors of PII required to register with the supervisory authority? Are there any exemptions?

There are no exemptions for registration for data users but only data users falling within the class of data users prescribed in the Personal Data Protection (Class of Data Users) Order 2013, which are largely limited to licensees within a particular sector, must register with the Personal Data Protection Commissioner (Commissioner). The sectors are:

- communications;
- banking and financial institutions;
- insurance;
- health;
- tourism and hospitality industries;
- transportation;
- education;
- direct selling;
- services (legal, audit, accountancy, engineering or architecture);
- real estate;
- utilities;
- pawnbrokers; and
- moneylenders.

Formalities

26 | What are the formalities for registration?

Applications for registration can be done online at https://daftar.pdp.gov.my/ and a registration fee is payable. Information required includes name and information of the company, purpose(s) of data collection, type(s) of data that will be collected, transfer of data out of Malaysia (if any), information of the person in charge of the registration, etc.

The documents required include incorporation documents, relevant licences etc. Any document as required by the Commissioner must also be submitted.

Registration certificates are valid for at least one year, after which data users must renew registrations.

Penalties

27 | What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

Data users falling under a prescribed class of data users required to register who process personal data without a registration certificate commit an offence and may be liable to a fine of up to 500,000 ringgit and imprisonment for up to three years.

Refusal of registration

28 | On what grounds may the supervisory authority refuse to allow an entry on the register?

The PDPA does not specify the grounds for refusal but the application for registration shall be deemed withdrawn if the applicant fails to provide any additional documents or information requested by the Commissioner in writing within the specified time. Where the Commissioner refuses the application for registration, he shall inform the applicant by a written notice that the application has been refused and the reasons for the refusal.

Public access

29 | Is the register publicly available? How can it be accessed?

The register is publicly available at https://daftar.pdp.gov.my/. Upon payment of the prescribed fee, any person may inspect the register or make a copy of or take extracts from an entry in the register.

Effect of registration

30 | Does an entry on the register have any specific legal effect?

The PDPA does not provide for any specific legal effect but failure to register (when so required) would attract penalties.

Other transparency duties

31 | Are there any other public transparency duties?

Not applicable.

TRANSFER AND DISCLOSURE OF PII

Transfer of PII

32 | How does the law regulate the transfer of PII to entities that provide outsourced processing services?

Persons other than the data user's employee who process personal data solely on the data user's behalf and not for their own purposes are considered 'data processors'.

In respect of data processors, data users must ensure that:

- Data processors provide sufficient guarantees in respect of the technical and organisational security measures governing the processing; and
- Reasonable steps are taken to ensure compliance with those measures, (eg, ensure constant monitoring in respect of the data processors' compliance with their guarantees).

The security standards set by the Personal Data Protection Commissioner (Commissioner) also require a contract to be established between a data user and the data processor. The security standards also prescribe certain security measures for electronic transfers. If the outsourcing involves the cross-border transfer of personal data, the Personal Data Protection Act 2010 (PDPA) prohibits such transfer except in certain circumstances. Other laws may impose further restrictions (eg, disclosure of banking account-related data is prohibited by our financial laws except in certain permitted circumstances).

Restrictions on disclosure

33 | Describe any specific restrictions on the disclosure of PII to other recipients.

A data user cannot disclose personal data without the individual's consent unless it is for the purpose it was collected for or if disclosure is to a third party which was specified in the notice to the data subject. A list of third-party disclosure must also be maintained.

Cross-border transfer

34 | Is the transfer of PII outside the jurisdiction restricted?

Cross-border transfer of personal data is prohibited unless it is to a gazetted place. A Public Consultation Paper No. 1/2017 on the Personal Data Protection (Transfer of Personal Data to Places Outside Malaysia) Order 2017 proposing the whitelisted countries has been issued but no country has yet to be gazetted as a permitted country.

Notwithstanding the prohibition, cross-border transfers are permissible in certain specified circumstances, among others:

- the individual's consent has been obtained;
- the transfer is necessary for the performance of a contract between the individual and the data user;
- the data user has taken all reasonable steps and exercised all due diligence to ensure the personal data will not be processed in a manner that would contravene the PDPA;
- the transfer is necessary for the purpose of legal proceedings or to obtain legal advice; and
- the transfer is necessary to protect the individual 's vital interest and for the public's interest.

Notification of cross-border transfer

35 | Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

There is presently no such requirement under the PDPA.

Further transfer

36 | If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

The PDPA does not distinguish between transfers to service providers and onwards transfer. The restrictions apply equally to both types of transfers.

RIGHTS OF INDIVIDUALS

Access

37 | Do individuals have the right to access their personal information held by PII owners? Describe how this right can be exercised as well as any limitations to this right.

Any cross-border transfers are prohibited unless it is to a gazetted place. A Public Consultation Paper No. 1/2017 on the Personal Data Protection (Transfer of Personal Data to Places Outside Malaysia) Order 2017 proposing the whitelisted countries has been issued but no country has yet to be gazetted as a permitted country.

Notwithstanding the prohibition, a cross-border transfer is permissible in certain specified circumstances, among others:

- the individual's consent has been obtained;
- the transfer is necessary for the performance of a contract between the individual and the data user;
- the data user has taken all reasonable steps and exercised all due diligence to ensure the personal data will not be processed in a manner that would contravene the PDPA;
- the transfer is necessary for the purpose of legal proceedings or to obtain legal advice;
- the transfer is necessary to protect the individual 's vital interest and for the public's interest;
- it will be against any court order;
- it will disclose confidential commercial information; or
- the access is regulated by another law.

Other rights

38 | Do individuals have other substantive rights?

The PDPA also confers the following rights on the individuals:

- the right to withdraw consent to process personal data;
- the right to prevent processing likely to cause damage or distress; and
- the right to prevent processing for direct marketing.

Compensation

39 | Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

The PDPA does not give the individuals the right to pursue civil claims against data users for breaching the PDPA.

Enforcement

40 | Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

Not applicable.

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

41 | Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

Not applicable.

SUPERVISION

Judicial review

42 | Can PII owners appeal against orders of the supervisory authority to the courts?

Data users aggrieved by the a decision of the Personal Data Protection Commissioner (Commissioner) may appeal to the Personal Data Protection Appeal Tribunal. The decisions that may be appealed are:

- decisions relating to the registration of data users;
- the refusal of the Commissioner to register a code of practice;
- the service of an enforcement notice;
- the Commissioner's refusal to vary or cancel an enforcement notice; and
- the Commissioner's refusal to conduct or continue an investigation based on a complaint.

If unsatisfied with the Personal Data Protection Advisory Committee's decision, the data user may file a judicial review in the Malaysian High Courts.

SPECIFIC DATA PROCESSING

Internet use

43 | Describe any rules on the use of 'cookies' or equivalent technology.

The Personal Data Protection Act 2010 (PDPA) does not have specific provisions on cookies or equivalent technology but such processing is subject to the PDPA's general provisions assuming the information collected contains personal data.

Electronic communications marketing

44 | Describe any rules on marketing by email, fax or telephone.

The individual has the right to require a data user to cease or not begin processing his personal data for direct marketing purposes. The definition of 'direct marketing' is broad enough to cover marketing by email, fax or telephone.

Marketing messages electronically transmitted are also governed by our telecommunications law. There are no specific provisions on the illegality of 'spam', but Section 233(1)(b) of the Communications and Multimedia Act 1998 (CMA) provides that:

> *[A] person who initiates a communication using any applications service, whether continuously, repeatedly or otherwise, during which communication may or may not ensue, with or without disclosing his identity and with intent to annoy, abuse, threaten or harass any person at any number or electronic address commits an offence.*

The Malaysian Communications and Multimedia Commission (MCMC) acknowledges that this provision may be inadequate in dealing with spam, but it should be ensured the marketing messages are not sent in a manner that contravenes this prohibition, (eg, sending messages repeatedly and continuously such that the intent to annoy, abuse, etc could be implied).

The MCMC also issued guidance on spamming, including:

- a public consultation report on 'Regulating Unsolicited Commercial Messages' dated 17 February 2004;
- FAQs on the MCMC website; and
- the Anti-spam Toolkit, which contains the Anti-Spam Framework of Best Practices and Technical Guidelines.

SKRINE

Jillian Chia Yan Ping
jc@skrine.com

Natalie Lim
natalie.lim@skrine.com

Level 8, Wisma UOA Damansara
50 Jalan Dungun, Damansara Heights
50490 Kuala Lumpur
Malaysia
Tel: +60 3 2081 3999
www.skrine.com

Generally, the main distinguishing factor between a legitimate message and spam is consent. The marketer must obtain the recipient's permission or consent before sending out marketing messages and the target audience should be those who have expressed an interest in a particular product or service being marketed by that sender. Whether the anti-spam rules are legally binding is unclear, but compliance would be good practice.

Cloud services

45 | Describe any rules or regulator guidance on the use of cloud computing services.

The use of cloud computing services is subject to the PDPA's general requirements, but the following security standards set by the Commissioner relate specifically to cloud services:

- The transfer of personal data using removable media device and cloud computing service is not allowed except with the written approval of an authorised officer from the upper management of data user's organisation.
- The transfer of personal data using removable media devices and cloud computing services must be recorded.
- That the transfer of personal data using cloud computing service must follow the personal data protection principles in Malaysia and other countries with personal data protection laws.

UPDATE AND TRENDS

Key developments of the past year

46 | Are there any emerging trends or hot topics in international data protection in your jurisdiction?

The Personal Data Protection Commissioner of the Ministry of Communications and Multimedia Malaysia has issued a proposal paper, Public Consultation Paper No. 01/2020 – Review of Personal Data Protection Act 2010 (PC01/2020) to seek the views and comments of the public, as part of an ongoing review of the Personal Data Protection Act 2010.

Other titles available in this series

Acquisition Finance
Advertising & Marketing
Agribusiness
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Appeals
Arbitration
Art Law
Asset Recovery
Automotive
Aviation Finance & Leasing
Aviation Liability
Banking Regulation
Business & Human Rights
Cartel Regulation
Class Actions
Cloud Computing
Commercial Contracts
Competition Compliance
Complex Commercial Litigation
Construction
Copyright
Corporate Governance
Corporate Immigration
Corporate Reorganisations
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Defence & Security Procurement
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
Drone Regulation
e-Commerce
Electricity Regulation
Energy Disputes
Enforcement of Foreign Judgments
Environment & Climate Regulation
Equity Derivatives
Executive Compensation & Employee Benefits
Financial Services Compliance
Financial Services Litigation
Fintech
Foreign Investment Review
Franchise
Fund Management
Gaming
Gas Regulation
Government Investigations
Government Relations
Healthcare Enforcement & Litigation
Healthcare M&A
High-Yield Debt
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Joint Ventures
Labour & Employment
Legal Privilege & Professional Secrecy
Licensing
Life Sciences
Litigation Funding
Loans & Secured Financing
Luxury & Fashion
M&A Litigation
Mediation
Merger Control
Mining
Oil Regulation
Partnerships
Patents
Pensions & Retirement Plans
Pharma & Medical Device Regulation
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Banking & Wealth Management
Private Client
Private Equity
Private M&A
Product Liability
Product Recall
Project Finance
Public M&A
Public Procurement
Public-Private Partnerships
Rail Transport
Real Estate
Real Estate M&A
Renewable Energy
Restructuring & Insolvency
Right of Publicity
Risk & Compliance Management
Securities Finance
Securities Litigation
Shareholder Activism & Engagement
Ship Finance
Shipbuilding
Shipping
Sovereign Immunity
Sports Law
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Technology M&A
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

lexology.com/gtdt

an LBR business

ISBN 978-1-83862-322-7