DATA PROTECTION & PRIVACY

Malaysia

LEXOLOGY
Getting The Deal Through

Consulting editor
Hunton Andrews Kurth LLP

Data Protection & Privacy

Consulting editors

Aaron P Simpson, Lisa J Sotto

Hunton Andrews Kurth LLP

Quick reference guide enabling side-by-side comparison of local insights into the legislative framework; relevant authorities; treatment of breaches; legitimate processing; data handling responsibilities of PII owners; security obligations; internal controls, including the data protection officer; registration formalities transfer and disclosure of PII; rights of individuals; judicial supervision; specific data processing use cases such as cookies, electronic communications marketing, and cloud services; and recent trends.

Generated 17 July 2023

Table of contents

Contributors

Malaysia

Jillian Chia Yan Ping
jc@skrine.com
SKRINE

Natalie Lim
natalie.lim@skrine.com
SKRINE

Beatrice Yew
beatrice.yew@skrine.com
SKRINE

LAW AND THE REGULATORY AUTHORITY

Legislative framework

Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions 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 (now replaced by the General Data Protection Regulation), came into force on 15 November 2013. The following subsidiary legislations have since been enacted under the PDPA:

- the Personal Data Protection Regulations 2013;
- the Personal Data Protection (Class of Data Users) Order 2013;
- the Personal Data Protection (Registration of Data User) Regulations 2013;
- the Personal Data Protection (Fees) Regulations 2013;
- the Personal Data Protection (Compounding of Offence) Regulations 2016; and
- the Personal Data Protection (Appeal Tribunal) Regulations 2021.

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 enforceable codes of practice for the following sectors have been registered:

- the utilities sector (electricity);
- the insurance or takaful industry;
- the banking and financial sector;
- the transportation sector (aviation);
- the communications sector;
- the utilities sector (water); and
- the private hospitals in the healthcare industry.

The Personal Data Protection Commissioner recently issued the General Code of Practice of Personal Data Protection (General COP), effective from 15 December 2022. The General COP applies to classes of data users who do not fall within the sectors listed above.

Law stated - 19 May 2023

Data protection authority

Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

As the responsible authority in Malaysia, the functions of the Personal Data Protection Commissioner (the 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 or her 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.

Law stated - 19 May 2023

Cooperation with other data protection authorities

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 provides 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 concerning their personal data.

Law stated - 19 May 2023

Breaches of data protection law

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.

Law stated - 19 May 2023

Judicial review of data protection authority orders

Can PI owners appeal to the courts against orders of the data protection authority?

Data users aggrieved by the Commissioner's decision may appeal to the Personal Data Protection Appeal Tribunal. The decisions that may be appealed are:

- decisions relating to the registration of data users;
- refusal of the Commissioner to register a code of practice;
- 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 Appeal Tribunal's decision, the data user may file a judicial review in the Malaysian High Courts.

Law stated - 19 May 2023

SCOPE

Exempt sectors and institutions

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 that is processed in respect of a 'commercial transaction' but certain sectors and types of processing are exempted, such as:

- the 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
- the processing of information by the Malaysian federal and state governments.

Law stated - 19 May 2023

Interception of communications and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

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 the 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 or her personal data for the purposes of 'direct marketing' (communication by any means that is directed to particular individuals).

The telecommunications and computer crimes laws also generally prohibit the 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 that prohibits communications initiated to annoy, abuse, threaten or harass a person.

Law stated - 19 May 2023

Other laws

Are there 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 that apply to financial and health data.

The Financial Services Act 2013 (FSA) prohibits the disclosure of any document or 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 (the BNM Guidelines) to govern data management by the financial sector. The BNM Guidelines apply 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.

Law stated - 19 May 2023

PI formats

What categories and types of PI 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. This includes '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 of Communications and Multimedia may determine by a gazette order. Such broad definition includes data in electronic and manual form.

Law stated - 19 May 2023

Extraterritoriality

Is the reach of the law limited to PI owners and processors physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

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.

Law stated - 19 May 2023

Covered uses of PI

Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI 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 or her 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.

Law stated - 19 May 2023

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

Does the law require that the processing of PI 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 to enter 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.

However, there are conditions for processing that the data user must comply with (regardless of whether consent or explicit consent has been obtained). Personal data must 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; and

- the personal data is adequate but not excessive concerning that purpose.

Law stated - 19 May 2023

Legitimate processing – types of PI

Does the law impose more stringent rules for processing specific categories and types of PI?

Stricter rules apply to the 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 of Communications and Multimedia 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:

- to exercise or perform any right or obligation that 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
- to obtain legal advice, or the establishment, exercising or defence of legal claims.

Law stated - 19 May 2023

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

A data user must inform 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.
-

In relation to bullet point (4) above, the Personal Data Protection Regulations 2013 provide that the data user must at least provide the data subject with the following details:

- designation of the contact person;
- phone number;
- fax number, if any;
- email address, if any; and
- such other related information.

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

- 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.

The Personal Data Protection Department recently issued the Guide to Prepare Personal Data Protection Notice (the Guide), which requires the following additional information or 'compulsory elements' to be stated in personal data protection notices:

- any sensitive personal data involved in processing;
- if personal data of children under 18 years old is processed;
- if there is any regulator requirement to collect certain personal data;
- how long the personal data will be retained in such processing;
- when the personal data be will disposed of;
- what practical measures will be taken to ensure personal data is secured;
- name of the person in charge in relation to how to contact data user for queries or complaints regarding personal data;
- the names of third parties to whom the personal data of data subject are shared with and for what purpose; and
- the security measures in place to ensure the disclosure implemented is safe and secure.

It remains uncertain at present whether the Guide is legally binding.

Law stated - 19 May 2023

Exemptions from transparency obligations

When is notice not required?

Notice is not required when personal data:

- is processed for the prevention or detection of crime or the purpose of investigations, apprehension or prosecution of offenders, or assessment or collection of any tax or duty or other similar impositions;
- is processed to prepare statistics or carry out research provided that the resulting statistics or research results are not in a form that 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.

Law stated - 19 May 2023

Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PI?

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 (the 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).

Law stated - 19 May 2023

Data minimisation

Does the law restrict the types or volume of PI that may be collected?

The Personal Data Protection Act 2010 (PDPA) does not restrict the types or volume of personal information that may be collected, but the General Principle in the PDPA prescribes that personal data must not be processed unless the personal data is adequate but not excessive in relation to the purpose for which it is processed.

Law stated - 19 May 2023

Data retention

Does the law restrict the amount of PI that may be held or the length of time for which PI 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, Malaysian 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 time frame (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 to the commercial transaction).

Law stated - 19 May 2023

Purpose limitation

Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

There are no express restrictions on the purposes for which PI can be used 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 is adequate and not excessive concerning that purpose. Processing must also be restricted to the

purposes described in the notice.

For new purposes, consent must be obtained again unless any of the exceptions to the consent requirement apply. The notice must also be amended to cater to the new purpose.

Law stated - 19 May 2023

Automated decision-making

Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

The PDPA does not currently contain any requirements or restrictions relating to automated decision-making.

Law stated - 19 May 2023

SECURITY

Security obligations

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

Data users must take practical steps to protect personal data from any loss, misuse, modification, unauthorised 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 Personal Data Protection Commissioner (the Commissioner). The following is a brief non-comprehensive overview of the prescribed security standards.

In respect of electronically processed personal data:

- 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 that 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 backup and recovery systems;
- to deploy the latest antivirus software and schedule malware monitoring and scanning of operating systems to prevent attacks on electronically stored data; and
- 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;
- to record the transfer of personal data using conventional methods such as through post, by hand, fax or others;
- to ensure that all used paper, printed documents or other documents that clearly show personal data must be properly destroyed; and
- to conduct awareness programmes on the responsibility to protect personal data for all relevant personnel (if necessary).

Law stated - 19 May 2023

Notification of data breach

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 and does not define 'data breach', but the authorities issued a public consultation paper in 2018, The Implementation of Data Breach Notification, which sought to introduce a data breach notification regime, where data users would be required to notify regulators and affected individuals in the event of a data breach. The consultation paper sets out, among other things:

- 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 programmes on data protection.

However, the consultation paper has yet to be gazetted as law.

While it is not a mandatory requirement under the PDPA, an online data breach notification to the Commissioner can be made. The required information includes:

- the particulars of the data user and the person giving the notification;
- the details of the data breach;
- containment and recovery; and
- notifications made to other parties (regulators and law enforcement agencies, affected parties, data processors, or other overseas data protection authorities).

Under this voluntary data breach notification regime, the data breach incident should be reported within 72 hours.

Law stated - 19 May 2023

INTERNAL CONTROLS

Accountability

Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

The Personal Data Protection Act 2010 (PDPA) does not have express accountability principles per se, but data users are required to develop and implement a security policy which is compliant with the security standards set by the Personal Data Protection Commissioner (the Commissioner).

To demonstrate compliance with the law, a data user must keep and maintain a record of any application, notice, request or any other information relating to personal data processed by them in the form and manner that may be determined by the 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, inter alia, record of consent and notice, list of disclosures to third parties and the security policy.

Law stated - 19 May 2023

Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

The PDPA does not presently mandate the appointment of a data protection officer.

However, pursuant to the Public Consultation Paper No. 01/2020 – Review of Personal Data Protection Act 2010 , dated 14 February 2020, the Commissioner is considering introducing an obligation in the PDPA for a data user to appoint a data protection officer and introduce a guideline pertaining to officers.

Law stated - 19 May 2023

Record-keeping

Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

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 or her in the form and manner that may be determined by the 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, a list of disclosures to third parties and the security policies. Other laws may also prescribe record-keeping requirements (eg, tax laws).

Law stated - 19 May 2023

Risk assessment

Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

The PDPA does not presently require data users to carry out risk assessments.

Law stated - 19 May 2023

Design of PI processing systems

Are there any obligations in relation to how PI processing systems must be designed?

The PDPA does not presently require data users to apply a privacy-by-design or privacy-by-default approach. However, pursuant to the Public Consultation Paper No. 01/2020 – Review of Personal Data Protection Act 2010, dated 14 February 2020, the Commissioner is considering a proposal to instruct that any new system is required to apply privacy by design and to issue a guideline on the mechanism.

Law stated - 19 May 2023

REGISTRATION AND NOTIFICATION

Registration

Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

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 (the 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.

Applications for registration can be done online and a registration fee is payable. Information required includes, inter alia, the name and information of the company and information of the person in charge of the registration. The documents required include, inter alia, incorporation documents and relevant licences. Any document as may be required by the Commissioner must also be submitted. Registration certificates are valid for at least one year, after which data users must renew registrations.

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 or imprisonment for up to three years, or both.

Law stated - 19 May 2023

Other transparency duties

Are there any other public transparency duties?

Not applicable.

Law stated - 19 May 2023

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

How does the law regulate the sharing of PI with 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 (the 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 (eg, consent has been obtained, the transfer is necessary for the performance of a contract between the data subject and the data user, or the data user has taken all reasonable precautions and exercised all due diligence to ensure that the personal data will not in that place be processed in any manner which, if that place is Malaysia, would be a contravention of the PDPA (among other exceptions)). Other laws may impose further restrictions (eg, disclosure of banking account-related data is prohibited by Malaysian financial laws except in certain permitted circumstances).

Law stated - 19 May 2023

Restrictions on third-party disclosure

Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

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

Law stated - 19 May 2023

Cross-border transfer

Is the transfer of PI outside the jurisdiction restricted?

Cross-border transfer of personal data is prohibited unless it is to a gazetted place. 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 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.

There are presently no supervisory authority notification or authorisation requirements for cross-border data transfers under the PDPA.

Law stated - 19 May 2023

Further transfer

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.

Law stated - 19 May 2023

Localisation

Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

There are no general data localisation requirements under the PDPA. However, there may be other laws or industry-specific rules that require this (eg, there may be requirements under tax and company law to maintain certain accounting reports and records relating to any business in Malaysia locally, as well as industry-specific laws to keep data within Malaysia, particularly in the financial services sector).

Law stated - 19 May 2023

RIGHTS OF INDIVIDUALS

Access

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

Under the Access Principle, a data subject has a right of access to his or her data and to correct it if it is inaccurate, incomplete, misleading or outdated.

Certain prescribed procedures have been set out where access or correction is requested by the data subject (ie, where the data subject requires a copy of the personal data, the data user must acknowledge receipt of the request). The Personal Data Protection Regulations 2013 also set out the information that may be requested by a data user when processing an access request.

Generally, a data user must comply with an individual's request to access and correct their personal data, except where:

- the data user is not supplied with sufficient information as to the identity of the requestor or of the relevant person making the request (information that may be requested includes identification card number and address);
- the data user is not supplied with sufficient information to enable him or her to locate the personal data;
- the burden or expense of providing access is not proportionate to the risk of the data subject's privacy;
- the data user cannot comply with the request without disclosing the personal data of another individual who is identifiable from that information (unless consent of that individual has been obtained or it is reasonable to comply without the consent of such other individual);
- the processing of personal data is controlled by another data user in a manner that prohibits the relevant data user from complying in whole or part with the request;
- it will be against any court order;
- it will disclose confidential commercial information; or
- the access is regulated by another law.

Law stated - 19 May 2023

Other rights

Do individuals have other substantive rights?

The Personal Data Protection Act (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.

Law stated - 19 May 2023

Compensation

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 individuals the right to pursue civil claims against data users for breaching the PDPA.

Law stated - 19 May 2023

Enforcement

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

Not applicable.

Law stated - 19 May 2023

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described?

Not applicable.

Law stated - 19 May 2023

SPECIFIC DATA PROCESSING

Cookies and similar technology

Are there 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.

Law stated - 19 May 2023

Electronic communications marketing

Are there any rules on marketing by email, fax, telephone or other electronic channels?

Under the PDPA, an individual has the right to require a data user to cease or not begin processing his or her 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 Malaysia's 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:

- the 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.

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.

Law stated - 19 May 2023

Targeted advertising

Are there any rules on targeted online advertising?

There are presently no specific rules on targeted online advertising under the PDPA.

Law stated - 19 May 2023

Sensitive personal information

Are there any rules on the processing of 'sensitive' categories of personal information?

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 of Communications and Multimedia 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 that 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 or exercise of defence of legal claims.

Law stated - 19 May 2023

Profiling

Are there any rules regarding individual profiling?

There are presently no specific rules on individual profiling under the PDPA.

Law stated - 19 May 2023

Cloud services

Are there 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 Personal Data Protection 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 the data user's organisation;
- the transfer of personal data using removable media devices and cloud computing services must be recorded; and
- 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.

Law stated - 19 May 2023

UPDATE AND TRENDS

Key developments of the past year

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

The Personal Data Protection Commissioner issued a proposal paper, Public Consultation Paper No. 01/2020 – Review of Personal Data Protection Act 2010 (PC01/2020), dated 14 February 2020, to seek the views and comments of the public as part of an ongoing review of the Personal Data Protection Act 2010 (PDPA). Some of the issues for which

feedback is sought include the extension of obligations to data processors, and providing the right to commence civil litigation against data users.

Based on past statements made by the Minister of Communications and Digital in news reports, we understand that the following five key areas are the focus of the amendments:

- appointment of a data protection officer;
- mandatory data breach notification;
- direct obligation on data processors to comply with the Security Principle;
- right to data portability; and
- removal of the white-list regime for cross-border transfer of personal data.

The draft amendment to the PDPA is expected to be presented in Parliament before the end of 2023.

Law stated - 19 May 2023

Jurisdictions

Australia	Piper Alderman
Austria	Knyrim Trieb Rechtsanwälte
Belgium	Hunton Andrews Kurth LLP
Brazil	Mattos Filho Veiga Filho Marrey Jr e Quiroga Advogados
Canada	.
Chile	Magliona Abogados
China	Mayer Brown
France	Aramis Law Firm
Germany	Hoffmann Liebs Fritsch & Partner
Greece	GKP Law Firm
Hong Kong	Mayer Brown
Hungary	VJT & Partners
India	AP & Partners
Indonesia	SSEK Law Firm
Ireland	Walkers
Italy	ICT Legal Consulting
Japan	Nagashima Ohno & Tsunematsu
Jordan	Nsair & Partners - Lawyers
Malaysia	SKRINE
Malta	Fenech & Fenech Advocates
New Zealand	Anderson Lloyd
Pakistan	S.U.Khan Associates Corporate & Legal Consultants
Poland	Kobylanska Lewoszewski Mednis
Portugal	Morais Leitao Galvao Teles Soares da Silva and Associados
Serbia	BDK Advokati

South Africa	Covington & Burling LLP
South Korea	Bae, Kim & Lee LLC
Switzerland	Lenz & Staehelin
Taiwan	Formosa Transnational Attorneys at Law
Thailand	Formichella & Sritawat Attorneys at Law
Turkey	Turunç
United Arab Emirates	Bizilance Legal Consultants
United Kingdom	Hunton Andrews Kurth LLP
USA	Hunton Andrews Kurth LLP