DATA PROTECTION LAWS OF THE WORLD

Malaysia

DLA PIPER

MALAYSIA

Last modified 21 December 2023

LAW

Malaysia's first comprehensive personal data protection legislation, the Personal Data Protection Act 2010 (PDPA), was passed by the Malaysian Parliament on June 2, 2010 and came into force on November 15, 2013.

As part of an ongoing review of the PDPA, the Personal Data Protection Commissioner of the Ministry of Communications and Multimedia Malaysia has issued Public Consultation Paper No. 01/2020 – Review of Personal Data Protection Act 2010 (PC01/2020) dated February 14, 2020 to seek the views and comments of the public on 22 issues set out in PC01/2020, some of which are set out below.

The Personal Data Protection Department (PDP Department) has indicated that, out of the 22 issues, 5 issues have been shortlisted as the key proposed amendments to the PDPA. In October 2023, the Deputy Minister of Communications, Teo Nie Ching, stated that the preparation of the bill to amend the PDPA is in the final stages, and she expected that the said bill will be tabled in March 2024.

DEFINITIONS

Definition of personal data

'Personal data' means any information in respect of commercial transactions that is:

- Being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose;
- Recorded with the intention that it should wholly or partly be processed by means of such equipment; or
- Recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, and, in each case.

...that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession of a data user.

Personal data includes any sensitive personal data or expression of opinion about the data subject. Personal data does not include any information that is processed for the purpose of a credit reporting business carried on by a credit reporting agency under the Credit Reporting Agencies Act 2010.

Definition of sensitive personal data

'Sensitive personal data' means any personal data consisting of information as to the physical or mental health or condition of a data subject, his or her political opinions, his or her religious beliefs or other beliefs of a similar nature, the commission or alleged

commission by him or her of any offense or any other personal data as the Minister of Communications and Multimedia (Minister) may determine by published order. Other than the categories of sensitive personal data listed above, the Minister has not published any other types of personal data to be sensitive personal data as of December 15, 2020.

NATIONAL DATA PROTECTION AUTHORITY

Pursuant to the PDPA, a Personal Data Protection Commissioner (Commissioner) has been appointed to implement the PDPA's provisions. The Commissioner will be advised by a Personal Data Protection Advisory Committee who will be appointed by the Minister, and will consist of one Chairman, three members from the public sector, and at least seven, but no more than eleven other members. The appointment of the Personal Data Protection Advisory Committee will not exceed a term of three years; however, members can be appointed for two successive terms.

The Commissioner's decisions can be appealed through the Personal Data Protection Appeal Tribunal. The following are examples of appealable decisions:

- Decisions relating to the registration of data users under Part II Division 2 of the PDPA;
- The refusal of the Commissioner to register a code of practice under Section 23(5) of the PDPA;
- The service of an enforcement notice under Section 108 of the PDPA;
- The refusal of the Commissioner to vary or cancel an enforcement notice under Section 109 of the PDPA; or
- The refusal of the Commissioner to conduct or continue an investigation that is based on a complaint under Part VIII of the PDPA.

If a data user is not satisfied with a decision of the Personal Data Protection Advisory Committee, the data user may proceed to file a judicial review of the decision in the Malaysian High Courts.

REGISTRATION

Currently, the PDPA requires the following classes of data users to register under the PDPA:

1. **Communications**
    - A licensee under the Communications and Multimedia Act 1998
    - A licensee under the Postal Services Act 2012
2. **Banking and financial institutions**
    - A licensed bank and licensed investment bank under the Financial Services Act 2013
    - A licensed Islamic bank and licensed international Islamic bank under the Islamic Financial Services Act 2013
    - A development financial institution under the Development Financial Institution Act 2002
3. **Insurance**
    - A licensed insurer under the Financial Services Act 2013
    - A licensed takaful operator under the Islamic Financial Services Act 2013
    - A licensed international takaful operator under the Islamic Financial Services Act 2013
4. **Health**
    - A licensee under the Private Healthcare Facilities and Services Act 1998
    - A holder of the certificate of registration of a private medical clinic or a private dental clinic under the Private Healthcare Facilities and Services Act 1998
    - A body corporate registered under the Registration of Pharmacists Act 1951
5. **Tourism and hospitalities**
    - A licensed person who carries on or operates a tourism training institution, licensed tour operator, licensed travel agent or licensed tourist guide under the Tourism Industry Act 1992
    - A person who carries on or operates a registered tourist accommodation premises under the Tourism Industry Act 1992
6. **Transportation**
    - Certain named transportations services providers
7. **Education**
    - A private higher educational institution registered under the Private Higher Educational Institutions Act 1996

- A private school or private educational institution registered under the Education Act 1996

8. **Direct selling**
    - A licensee under the Direct Sales and Anti-Pyramid Scheme Act 1993
9. **Services**
    - A company registered under the Companies Act 1965 or a person who entered into partnership under the Partnership Act 1961 carrying on business as follows:
        - legal
        - audit
        - accountancy
        - engineering
        - architecture
    - A company registered under the Companies Act 1965 or a person who entered into partnership under the Partnership Act 1961, who conducts retail dealing and wholesale dealing as defined under the Control Supplies Act 1961
    - A company registered under the Companies Act 1965 or a person who entered into partnership under the Partnership Act 1961, who carries on the business of a private employment agency under the Private Employment Agencies Act 1981
10. **Real estate**
    - A licensed housing developer under the Housing Development (Control and Licensing) Act 1966
    - A licensed housing developer under the Housing Development (Control and Licensing) Enactment 1978, Sabah
    - A licensed housing developer under the Housing Developers (Control and Licensing) Ordinance 1993, Sarawak
11. **Utilities**
    - Certain named utilities services providers
12. **Pawnbroker**
    - A licensee under the Pawnbrokers Act 1972
13. **Moneylender**
    - A licensee under the Moneylenders Act 1951

Certificates of registration are valid for at least one year, after which data users must renew registrations and may not continue to process personal data.

Data users are also required to display their certificate of registration at a conspicuous place at their principal place of business, and a copy of the certificate at each branch, where applicable.

The Commissioner may designate a body as a data user forum for a class of data users. Data user forums can prepare codes of practice to govern compliance with the PDPA, which can be registered with the Commissioner. Once registered, all data users must comply with the provisions of the code, and non-compliance violates the PDPA. As of December 20, 2023, the Commissioner has published several codes of practice, including for the banking and financial sector, the aviation sector, the utilities sector, communications sector, the healthcare sector, and the insurance and takaful industry in Malaysia. There is also a general code of practice which applies to classes of data users required to be registered as data users under the PDPA who are currently not subject to any codes of practice registered by the Commissioner.

DATA PROTECTION OFFICERS

Currently, Malaysian law does not require that data users appoint a data protection officer.

However, pursuant to PC01/2020, the Commissioner is considering introducing an obligation in the PDPA for a data user to appoint a data protection officer and to introduce a guideline pertaining to such appointments.

The PDP Department has indicated that this requirement has been shortlisted as one of the five key proposed amendments to the PDPA which were under consideration (out of the 22 issues set out in P01/2020).

COLLECTION & PROCESSING

Under the PDPA, subject to certain exceptions, data users are generally required to obtain a data subject’s consent for the processing (which includes collection and disclosure) of his or her personal data. Where consent is required from a data subject under the age of eighteen, the data user must obtain consent from the parent, guardian or person who has parental responsibility for the data subject. The consent obtained from a data subject must be in a form that such consent can be recorded and maintained properly by the data user.

Pursuant to PC01/2020, the Commissioner has sought feedback on its proposal to amend the General Principle provision to add clarity to the data subject's consent, whether it should be in a specific provision and the impact of having a default consent.

Malaysian law contains additional data protection obligations, including, for example, a requirement to notify data subjects regarding the purpose for which their personal data are collected and a requirement to maintain a list of any personal data disclosures to third parties.

On December 23, 2015, the Commissioner published the Personal Data Protection Standard 2015 ("**Standards**"), which set out the Commission’s minimum requirements for processing personal data. The Standards include the following:

- Security Standard For Personal Data Processed Electronically
- Security Standard For Personal Data Processed Non-Electronically
- Retention Standard For Personal Data Processed Electronically And Non-Electronically
- Data Integrity Standard For Personal Data Processed Electronically And Non-Electronically

TRANSFER

Under the PDPA, a data user may not transfer personal data to jurisdictions outside of Malaysia unless that jurisdiction has been specified by the Minister. However, there are exceptions to this restriction, including the following:

- The data subject has given his or her consent to the transfer;
- The transfer is necessary for the performance of a contract between the data subject and the data user;
- The data user has taken all reasonable steps and exercised all due diligence to ensure that the personal data will not be processed in a manner that would contravene the PDPA; and
- The transfer is necessary to protect the data subject’s vital interests.

In 2017, the Commissioner published a draft Personal Data Protection (Transfer of Personal Data to Places Outside Malaysia) Order 2017 to obtain public feedback on the proposed jurisdictions to which personal data from Malaysia may be transferred. As of December 15, 2020, the Minister has yet to approve the safe harbor jurisdictions. Once approved, a data user may transfer personal data to these safe harbor jurisdictions without having to rely on the data subject's consent or other prescribed exceptions under the PDPA.

Pursuant to PC01/2020, the Commissioner acknowledged that a clear provision and the conditions for transferring personal data to places outside Malaysia are essential to facilitate e-commerce transactions and free trade agreements, and opined that a whitelist appears to curb and set a barrier for data users to transfer personal data to places outside Malaysia. In view of this, the Commissioner is considering restructuring the provision on cross border transfers under the PDPA and removing the whitelist provision. In this regard, the PDP Department has indicated that the whitelist regime will be replaced with a blacklist regime, where data users will generally be allowed to transfer personal data out of Malaysia (except to countries that have been blacklisted by the Minister).

In addition, the Commissioner also acknowledged that data users with overseas branches may need to exchange information with its branches at some point. The Commissioner is considering issuing a guideline on the mechanism and implementation of cross border data transfer and has sought feedback on the important matters to be considered in the proposed guideline.

SECURITY

Under the PDPA, data users have an obligation to take ‘practical’ steps to protect personal data, and in doing so, must develop and implement a security policy. The Commissioner may also, from time to time, set out security standards with which the data user must comply, and the data user is required to ensure that its data processors comply with these security standards.

In addition, the Standards provide separate security standards for personal data processed electronically and for personal data processed non-electronically (among others) and require data users to have regard to the Standards in taking practical steps to protect the personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction.

Pursuant to PC01/2020, the Commissioner observed that there are many new technologies such as facial recognition and smart trackers being used as data collection endpoints, and thus is considering issuing a policy regarding the endpoint security which uses technologies such as encryption. Additionally, it may be of interest to note that the PDP Department has indicated that the proposed amendment bill may impose a direct obligation on data processors to comply with the Security Principle under the PDPA.

BREACH NOTIFICATION

Currently, there is no requirement under the PDPA for data users to notify authorities regarding data breaches in Malaysia. Previously there was a voluntary data breach notification option available on the PDP Department’swebsite, but the option appears to be no longer available. News reports dated October 5, 2018 suggest that Malaysia's laws could be updated, to include data breach notification requirements modeled after those under the European Union's General Data Protection Regulation (GDPR), including requiring providing notice to government authorities.

In addition, a news report dated March 20, 2019 reported that the Office of Personal Data Protection Malaysia's deputy commissioner, Rosmahyuddin Baharuddin, has also indicated that data breach notification is something that Malaysia is "seriously considering".

Notably, one of the issues for which feedback is sought in P01/2020 include reporting of data breaches. The points to be considered include, the proposed mandatory data breach notification, the impact of having all data users report about the data, and the elements to be considered in the guideline on data breach incident reporting. The PDP Department has indicated that data breach notification is shortlisted as one of the five key proposed amendments to the PDPA which is under consideration.

ENFORCEMENT

Under the PDPA, the Commissioner is empowered to implement and enforce the personal data protection laws and to monitor and supervise compliance with the provisions of the PDPA. Under the Personal Data Protection Regulations 2013, the Commissioner has the power to inspect the systems used in personal data processing and the data user is required, at all reasonable times, to make the systems available for inspection by the Commissioner or any inspection officer. The Commissioner or the inspection officers may require the production of the following during inspection:

- The record of the consent from a data subject maintained in respect of the processing of that data subject's personal data by the data user;
- The record of required written notices issued by the data user to the data subject;
- The list of personal data disclosures to third parties;
- The security policy developed and implemented by the data user;
- The record of compliance with data retention requirements;
- The record of compliance with data integrity requirements; and
- Such other related information which the Commissioner or any inspection officer deems necessary.

Violations of the PDPA and certain provisions of the Personal Data Protection Regulations 2013 are punishable with criminal liability. The prescribed penalties include fines, imprisonment or both. Directors, CEOs, managers or other similar officers will have joint and several liability for non-compliance by the body corporate, subject to a due diligence defense.

There is no express right under the PDPA allowing aggrieved data subjects to pursue a civil claim against data users for breaches of the PDPA.

However, under PCP 01/2020, the Commissioner has proposed to introduce a specific provision stating the right of a data subject to commence civil litigation against a data user.

ELECTRONIC MARKETING

The PDPA applies to electronic marketing activities that involve the processing of personal data for the purposes of commercial transactions. There are no specific provisions in the PDPA that deal with electronic marketing. However, the PDPA provides that a data subject may, at any time by notice in writing to a data user, require the data user at the end of such period as is reasonable in the circumstances to cease or not to begin processing his or her personal data for direct marketing purposes. 'Direct marketing' means the communication by whatever means of any advertising or marketing material that is directed to particular individuals.

Pursuant to PCP 01/2020, the Commissioner is considering issuing a guideline to data users on the mechanism of digital and electronic marketing. The Commissioner has sought feedback on a proposed requirement on data users to provide a clear mechanism for data subjects to unsubscribe from online services and the elements to be considered in preparing the guideline on processing personal data in digital and electronic marketing.

The Commissioner is also considering issuing a guideline on the implementation of direct marketing for data users. Feedback from the public is sought as to whether a proposed data user is allowed to make the first direct marketing call to the data subject, the use of the 'opt-out' method, and the important elements to be considered in the preparation of such guideline.

ONLINE PRIVACY

There are no provisions in the PDPA that specifically address the issue of online privacy (including cookies and location data). However, any electronic processing of personal data in Malaysia will be subject to the PDPA and the Commissioner may issue further guidance on this issue in the future.

KEY CONTACTS

Skrine
www.skrine.com/

Jillian Chia
Partner
Skrine
T + 603 2081 3882
jc@skrine.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.