NEWSLETTER

A Sea Change in Malaysia's Data Protection Framework
– Personal Data Protection (Amendment) Act 2024 and Public Consultation Papers –

Asia & Data Protection Newsletter November 22, 2024

Author:
Wan May Leong
w.m.leong@nishimura.com
Ryan Heng
ryan.heng@wmlaw.com.my
Wai Kin Leo
waikin.leo@wmlaw.com.my
Tomonobu Murata
to.murata@nishimura.com

On 17 October 2024, the Personal Data Protection (Amendment) Act 2024 ("**Amendment Act**") was announced in the official Gazette. The Amendment Act will become effective on a date to be announced by the Minister of Digital in the official Gazette.

The Amendment Act seeks to update and enhance the Personal Data Protection Act 2010 ("**PDPA**") by strengthening security and enforcement policies to more effectively address personal data breaches and misuse. These proposed changes are being introduced to ensure that Malaysia's data protection framework remains robust and aligned with international best practices.

Apart from the revision of terminology from "data users" to "data controllers," the key changes proposed in the Amendment Act are as follows.

1. Increased penalties

Currently, non-compliance with the PDPA carries a potential fine of up to RM 300,000 (approx. USD $68,508) and/or imprisonment for a term not exceeding two years.

The Amendment Act seeks to increase the penalties for a data controller's non-compliance with any of the seven personal data protection principles to a potential fine of up to RM 1,000,000 (approx. USD $228,336) and/or imprisonment for a term not exceeding three years (collectively, the "**Increased Penalties**").

2. Requirements for Data Processors to Comply With the Security Principle

Currently, the PDPA imposes data protection obligations only on data users, not on data processors. The Amendment Act proposes to extend certain obligations to data processors, including a requirement that they comply with the PDPA's security principle. As a result, data processors will be legally required to take practical steps to protect personal data against loss, misuse, modification, unauthorized or accidental access or disclosure, alteration, or destruction.

If a data processor fails to comply with the security principle, it will be subject to the Increased Penalties in the Amendment Act.

3. Mandatory Data Breach Notifications

The Amendment Act also seeks to require data controllers to notify the Personal Data Protection Commissioner ("**PDPC**") as soon as practicable if they have reason to believe that a personal data breach has occurred. The notification is to be made in the manner and form determined by the PDPC. Non-compliance with this requirement carries a potential fine not to exceed RM 250,000 (approx. USD $57,084) and/or imprisonment for a term not exceeding 2 years.

In addition, where a personal data breach causes or is likely to cause significant harm to the impacted data subject(s), the data controller is required to notify the impacted data subject(s) of the personal data breach, in the manner and form determined by the PDPC, without unnecessary delay.

For reference, the Amendment Act defines a "personal data breach" as any breach of personal data, loss of personal data, misuse of personal data, or unauthorized access to personal data.

4. Mandatory Appointment of Data Protection Officer

The Amendment Act requires every data controller and data processor to appoint at least one data protection officer, who is accountable to the relevant data controller/processor for compliance with the PDPA. Data controllers must notify the PDPC of the appointed data protection officer, in the manner and form determined by the PDPC.

The Amendment Act also clarifies that appointment of a data protection officer does not discharge a data controller/processor from the obligation to comply with all duties and functions required by the PDPA.

5. Changes to Cross-Border Data Transfer Regime

The PDPA currently prohibits transfers of personal data to locations outside of Malaysia (with certain exceptions), unless the destination is whitelisted by the Minister via a notification published in the Gazette. To date, no country has been officially whitelisted by the Minister.

The Amendment Act will remove the Minister's power to issue a data transfer whitelist. Instead, a data controller may transfer the personal data of a data subject to a location outside Malaysia, provided that:

(i) the destination has laws in force that are substantially similar to the PDPA; or

(ii) the destination ensures an adequate level of protection for the processing of personal data, equivalent to the level of protection afforded by the PDPA.

6. New Right to Data Portability

The Amendment Act also introduces a new right for data subjects to request that a data controller transmit the data subject's personal data directly to another data controller of the data subject's choice, when the data subject gives the data controller notice of the exercise of the right in writing, by electronic means. The data portability right and requirement is subject to technical feasibility and compatibility of data formats.

7. Other Notable Changes

The Amendment Act also proposes to expand the definition of "sensitive personal data" to include biometric data. Biometric data is defined in the Amendment Act as any personal data resulting from technical processing relating to the physical, physiological, or behavioral characteristics of a person.

The Amendment Act also seeks to exclude deceased individuals from the definition of "data subject" under the PDPA. The amendment by implication means that processing the personal data of a deceased individual is not subject to the PDPA.

Public Consultation Papers Issued by the Malaysian Department of Personal Data Protection

In January 2024, the Minister of Digital announced that the following guidelines will be developed by the Malaysian Department of Personal Data Protection ("**JPDP**"):

(i) Notification of Data Breach Guidelines;
(ii) Data Protection Officers Guidelines;
(iii) Data Portability Guidelines;
(iv) Cross Border Data Transfer Guidelines and Mechanism;
(v) Data Protection Impact Assessment Guidelines;
(vi) Privacy by Design Guidelines; and
(vii) Profiling and Automated Decision Making Guidelines.

Since then, the JPDP has issued public consultation papers to seek public feedback on the proposed guidelines identified in items (i), (ii), (iii), and (iv) above, as well as the proposed replacement of the Personal Data Protection Standard 2015 with a new set of security, retention, and data integrity standards.

In this newsletter, we have highlighted the following proposals discussed in the public consultation paper on the proposed Cross-Border Personal Data Transfer Guidelines ("**Cross-Border Transfer Consultation Paper**").

Cross-Border Transfer Consultation Paper

The PDPA (as amended by the Amendment Act) has established various legal bases for transferring personal data outside Malaysia. The Cross-Border Transfer Consultation Paper outlines the key considerations taken by the PDPC in developing the Cross-Border Personal Data Transfer Guidelines and clarifies the application of these legal bases as follows.

No.	Legal basis for the transfer of personal data outside Malaysia	Considerations and proposals discussed in the Cross-Border Transfer Consultation Paper
1.	There is in that place in force any law which is substantially similar to the PDPA.	Data controllers who seek to rely on this basis are required to carry out a Transfer Impact Assessment ("**TIA**") on the destination country to identify and assess the risks associated with a transfer of personal data to that country. The TIA should be used to determine whether any of the following

No.	Legal basis for the transfer of personal data outside Malaysia	Considerations and proposals discussed in the Cross-Border Transfer Consultation Paper
		exist/are in place: (a) similar data subject rights (e.g., right to access and right to correct) to those under the PDPA; (b) similar personal data protection principles to those under the PDPA; (c) similar protections on processing, disclosure, cross-border transfer, etc., to those under the PDPA; (d) similar requirements on data protection officers and data breach notification requirements to those under the PDPA; and (e) similar penalties and enforcement mechanisms to those under the PDPA to address data breaches.
2.	That place ensures at least equivalent level of protection afforded by the PDPA.	Data controllers who seek to rely on this basis are required to, among other matters, determine whether there are sufficient mechanisms in place to safeguard personal data, and carry out a TIA to determine whether the recipient: (a) has security measures and policies in place that are in line with the requirements of the PDPA; (b) has any security-related certifications; and (c) is bound by legal obligations and whether such obligations can be enforced by the data controller or data subjects.
3.	The data subject has given their consent to the transfer.	Data controllers who seek to rely on this basis are required to inform the data subjects of the cross-border transfer (such as via a privacy policy), including information such as the third parties who may have access to the personal data and the purpose of such transfer. The data's subject consent obtained must be recorded and kept on file.
4.	The transfer is necessary to achieve the stated purposes such as: (a) for the performance of a contract between the data subject and the data controller; (b) for the conclusion of performance of a contract between the data controller and a third party which: (i) is entered into at the request of the data subject; or (ii) is in the interests of the data subject; and to protect the vital interests of the data subject.	Data controllers who seek to rely on this basis are required to evaluate the following matters to determine whether a cross-border data transfer is necessary to achieve the stated purposes: (a) the cross-border transfer must be for a specific reason (rather than it being generally useful to the data controller and/or data subject), and it should not be a standard practice carried out by the data controller; (b) the cross-border transfer is made to achieve a specified purpose and not for a broader general purpose; and (c) the data controller cannot reasonably achieve the specified purpose through alternative means.
5.	The data controller has taken all reasonable precautions and exercised	Data controllers who seek to rely on this basis should adopt any of the following mechanisms as proof of compliance:

No.	Legal basis for the transfer of personal data outside Malaysia	Considerations and proposals discussed in the Cross-Border Transfer Consultation Paper
	all due diligence to ensure that the personal data will not, at the hands of the transferees, be processed in any manner which, if that place is Malaysia, would be a contravention of the PDPA.	(a) binding corporate rules (i.e., data protection rules that apply to intra-group cross-border data transfers); (b) standard contractual clauses (i.e. standard clauses that must be included in a contract between transferor and transferee to regulate the cross-border transfer); or (c) the transferee of personal data (i) has been issued a valid certificate recognised by the PDPC and (ii) has provided a guarantee to the data controller or processor to implement appropriate safeguards to protect the personal data.

Conclusion

The Amendment Act represents a significant step forward in that it more closely aligns the PDPA with global standards like the European Union's General Data Protection Regulation and strengthens Malaysia's commitment to personal data protection. It also is evidence of the Malaysian government's efforts to increase foreign investments in Malaysia's digital economy, particularly the data center services sector.

Once the Amendment Act and its guidelines come into force, businesses should review and update their existing data protection policies and practices, as well as data transfer/sharing/processing agreements, to ensure they are in compliance with the new requirements.

Public Relations Section, Nishimura & Asahi newsletter@nishimura.com