NEWSLETTER

# A Sea Change in Malaysia's Data Protection Framework (Part 2)

– The coming into force of the Personal Data Protection (Amendment) Act 2024 –

Asia & Data Protection Newsletter February 4, 2025

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

There have been several developments in the amendments to the Malaysian Personal Data Protection Act 2010 ("**PDPA**") since our previous newsletter on the topic which can be accessed here.

## The Amendment Act Comes Into Effect in Malaysia

On 24 December 2024, the Minister of Digital of Malaysia designated the dates on which the provisions of the Personal Data Protection (Amendment) Act 2024 ("**Amendment Act**") will come into force, by publishing a notification in the gazette.[1]

The Amendment Act will be implemented in 3 stages. The dates on which the amendments to the Amendment Act[2] have or will come into force are as follows:

(i) **1 January 2025** - Sections 7, 11, 13 and 14 of the Amendment Act. These amendments do not impose any new or particular obligations on data controllers.

(ii) **1 April 2025** - Sections 2, 3, 4, 5, 8, 10 and 12 of the Amendment Act. The salient amendments to the PDPA in this phase include:

(a) Replacement of the term "data user" with data controller."

(b) Extension of the obligation to comply with the security principle to data processors.
This means that a data processor that processes personal data on behalf of a data controller is required to take practical steps to protect the personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction, effective 1 April 2025.

(c) Increased penalties for breach of the personal data protection principles, including fines of up to RM 1,000,000 and/or imprisonment up to 3 years.

(d) Changes to the cross-border data transfer regime.
In short, a data controller may transfer personal data to a location outside Malaysia, provided that the destination has laws substantially similar to the PDPA or ensures an adequate level of personal data protection equivalent to the PDPA.

(iii) **1 June 2025** – Sections 6 and 9 of the Amendment Act. The salient amendments to the PDPA in this phase include:

1 https://www.pdp.gov.my/ppdpv1/wp-content/uploads/2024/12/PENETAPAN-TARIKH-PERMULAAN-KUAT-KUASA-1.pdf

2 PDP (Amendment)Act 2024 • Perlindungan Data Peribadi

(a) Mandatory appointment of a data protection officer by each data controller and data processor.
(b) Mandatory filing of data breach notification with the Personal Data Protection Commissioner ("**PDPC**").
(c) New right of data portability for data subjects.

## Timeline for Issuance of Guidelines and Revised Standards

The PDPC previously announced the release of the guidelines and standard by early 2025. However, as of the date of this newsletter, neither the guidelines on data protection officer, data breach notification, and cross border data transfer, nor the revised Personal Data Protection Standard, have been published. The remaining guidelines, including the guidelines on data protection impact assessment, are expected to be released during the third quarter of 2025.[3]

## Public Consultation Paper on Revised Personal Data Protection Standards

This newsletter will review the following proposals, which are addressed in the public consultation paper on the Personal Data Protection Standard[4] ("**Revised Standards Consultation Paper**").

Currently, the Personal Data Protection Standard 2015 (issued by the PDPC in 2015)[5] ("**Standards**") set out the security, retention, and data integrity standards which represent the minimum compliance standards for security, retention, and data integrity principles in the PDPA. The PDPC is updating the Standards, to introduce a revised set of security, retention, and data integrity standards in line with international best practices.

| No. | Concept Addressed in the Revised Standards Consultation Paper | Proposals in the Revised Standards Consultation Paper |
|---|---|---|
| 1. | Introduction of outcome-based standards | Currently, the Standards primarily consist of "black and white" rules, which set out specific and prescriptive instructions or measures with which data controllers must comply.<br>The PDPC proposes to replace these rules with requirements that are drafted using a more outcome-based approach, which will focus on defining the PDPC's expectations and outcomes that data controllers should attempt to achieve.<br>The amended Standards also will adopt a risk-based approach, to ensure that the measures implemented to meet various "outcomes" are proportionate to the level of risk faced by the organization. |
| 2. | Areas governed by the Security | Currently, the Standards established security standards that must be complied with depending on whether personal data was processed electronically or |

[3] https://www.pdp.gov.my/ppdpv1/en/pdp-commissioner-futurise-on-track-to-complete-guidelines-andstandard-under-the-act-709-by-the-end-of 2024/

[4] https://drive.google.com/file/d/1aWEcoAAZZiGy2ZC7CIfLNTJZThql7qOZ/view

[5] https://www.pdp.gov.my/ppdpv1/wp-content/uploads/2024/07/LatestStandard.pdf

| | | |
|---|---|---|
| | Standards | non-electronically. The PDPC proposes to remove this differentiation.<br>In addition, the PDPC proposes to establish a more comprehensive framework of security outcomes applicable to data controllers and data processors, which includes the following key elements: (a) governance structure, (b) access control, (c) asset and data inventory management, (d) protection against digital threats, (e) network security and software updates, (f) third party risk management, and (g) training / awareness. |
| 3. | Areas governed by the Retention Standards | The current retention standards primarily cover measures relating to the establishment of retention periods and preparation of records of disposal of personal data.<br>The PDPC proposes to expand the retention standards further, by referencing the following key elements: (a) duration of retention period, (b) documentation and records for retention and disposal of personal data, (c) methods of destruction or deletion of personal data, and (d) third-party retention of personal data. |
| 4. | Areas under the Data Integrity Standards | The current data integrity standards are not sufficiently comprehensive in terms of the measures that should be taken by data controllers to ensure that personal data is accurate, complete, not misleading, and kept up to date.<br>The PDPC's proposal for revising the data integrity standards will address the following key elements: (a) data validation and verification, (b) monitoring of data quality, (c) data consistency (e.g., implementing internal practices and procedures to ensure personal data is collected and recorded in a standardized and compatible format), and (d) data lifecycle management (e.g., promptly updating or adding new personal data to relevant existing records). |
| 5. | Role of certification programs to demonstrate compliance with the Standards | The PDPC proposes that industry certifications be recognized as a method that data controllers or data processors can use to demonstrate compliance with the Standards.<br>While obtaining an industry certification does not automatically imply blanket compliance or create immunity from sanctions or liabilities under the Standards, the PDPC will consider it a mitigating factor when assessing a data controller or data processor's compliance with the PDPA and the Standards. |

## Conclusion

When the relevant requirements in the Amendment Act come into force, businesses will be required to take specific actions to ensure compliance. These actions include the appointment of a data protection officer (by both data controllers and data processors), and compliance with the security principle by data processors. Where necessary, businesses should review and update their data protection practices to align with the requirements set forth in the Amendment Act.

In order to respond to the business needs of our clients, we publish newsletters on a variety of timely topics. Back numbers can be found here. If you would like to subscribe to the N&A Newsletter, please fill out the N&A Newsletter subscription form.



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