



## Introduction

The Personal Data Protection (Amendment) Act 2024 (“**Amendment Act**”), which represents the first legislative update to the Personal Data Protection Act 2010 (“**PDPA**”) since it became effective on 15 November 2013, will be implemented in three phases during the first half of 2025, beginning on 1 January 2025, followed by 1 April 2025 and 1 June 2025. The Amendment Act received Royal Assent on 9 October 2024 and was published in the Federal Gazette on 17 October 2024, following its passage by the House of Representatives and the Senate of Malaysian Parliament on 16 and 31 July 2024, respectively.

## First phase: 1 January 2025

The first phase of the amendments, which is poised to take effect on 1 January 2025, is generally administrative in nature. These amendments are amongst others as follows:

- a. that the procedure for opening, operating and maintaining any bank accounts for the personal data protection fund established under the PDPA, is to be carried out in the manner authorized by the Personal Data Protection Commissioner (“**Commissioner**”) (rather than by the Minister of Digital);
- b. that a service of a notice or any other document upon any person may also be effected by electronic means (in addition to the existing methods of hand delivery, leaving it at the last-known address or sending it by A.R. registered post);

- c. that any order, directions, circular, notice or code of practice issued by the Commissioner before the commencement of the Amendment Act will remain valid; and
- d. that any investigation, trial, proceedings or action that is ongoing before 1 January 2025 will continue under the original provisions of the PDPA and will not be affected by the amendments under the Amendment Act.

### **Second phase: 1 April 2025**

The second batch comprises the following key amendments, set to come into force on 1 April 2025:

- a. global change of the term “data user(s)” to the term “data controller(s)”;
- b. expansion of the definition of “sensitive personal data” to include “biometric data”, which means any personal data resulting from technical processing relating to the physical, physiological or behavioural characteristics of a person;
- c. a new definition for “personal data breach” which means any breach of personal data, loss of personal data, misuse of personal data or unauthorized access of personal data;
- d. exclusion of personal data of a deceased individual from the scope of the PDPA;
- e. expansion of the definition of “requestor” to include an individual who makes a data portability request;
- f. empowering the Commissioner to designate not only a body but also a data controller as a data controller forum in respect of a specific class of data controllers;
- g. a direct obligation on data processor to comply with the Security Principle when processing personal data on behalf of a data controller, including imposition of penalties on the data processor for breaching the Security Principle, with a fine of up to RM1 million and/or imprisonment for up to 3 years;
- h. an increased penalty rate for the offence committed by a data controller for breaching the Personal Data Protection Principles, to a fine of up to RM1 million (previously RM300,000) and/or a term of imprisonment of up to 3 years (previously 2 years); and

- i. allowing the transfer of personal data to a place outside Malaysia if there is in that place in force any law which is substantially similar to the PDPA, or that place ensures an adequate level of protection in relation to the processing of personal data which is at least equivalent to the level of protection afforded by the PDPA. There is no longer a white-list regime for cross-border data transfer.

### **Third phase: 1 June 2025**

The third phase of amendments will become effective on 1 June 2025 and includes the following:

- a. a new obligation on both data controller and data processor to appoint one or more data protection officers (“**DPO**”), with the data controller required to notify the Commissioner of the appointment;
- b. a new obligation on data controller to notify the Commissioner of a personal data breach as soon as practicable, and if the breach causes or likely to cause any significant harm to the data subject, to notify the data subject, failing which may result in a fine of up to RM250,000 and/or imprisonment for up to 2 years; and
- c. a new right of data portability for data subject who may request that his personal data be transmitted to another data controller of his choice, subject to technical feasibility and compatibility of the data format.

### **New regulations and guidelines**

The Commissioner is formulating new regulations and guidelines to complement the amendments to the PDPA, which are expected to be issued in tandem with the implementation of the Amendment Act. The Commissioner has previously released public consultation papers to gather feedback on these supplementary regulations and guidelines:

- a. Personal Data Protection (Personal Data Breach Notification) Regulations and Data Breach Notification Guideline (see [Public Consultation Paper No. 01/2024](#)), which seek to address:
  - i. notification thresholds for data breach notification (“**DBN**”) to the Commissioner (with proposals to clarify that the DBN requirement applies only in cases where the breach is likely to cause or have caused significant harm and/or where the

- breach is likely to be or is of a significant scale, taking into account certain factors);
- ii. notification thresholds for DBN to affected data subjects (with proposals to clarify what constitutes “significant harm”);
  - iii. manner and form of DBN to the Commissioner (with proposals to adopt the current template for voluntary notification, with appropriate modifications to simplify the content and presentation style and standardize the required response);
  - iv. manner and form of DBN to affected data subjects (with proposals mandating the minimum information to be provided in the notification);
  - v. timeframe for DBN to the Commissioner (with proposals requiring notification within 72 hours of becoming aware of the breach);
  - vi. timeframe for DBN to affected data subjects (with proposals to clarify that “without unnecessary delay” means at the same time as the notification to the Commissioner or as soon as practicable thereafter);
  - vii. exemptions from providing DBN to affected data subjects (with proposals to exclude the DBN requirement in cases where a data controller has implemented appropriate technological and organizational protection measures that renders it unlikely that the breach will result in significant harm to affected data subjects, or where the personal data compromised or affected by the breach is protected by security measures that make the information unintelligible or meaningless to unauthorized individuals);
  - viii. data processor’s obligation to comply with the DBN requirement (with proposals to contractually obligate the data processor to promptly notify the data controller of any personal data breach and provide all reasonable and necessary assistance);
  - ix. concurrent application of the DBN regime under the PDPA with other laws or sector-specific breach notification regimes (with proposals for the PDPA’s DBN regime to operate separately and concurrently with other relevant DBN requirements imposed under other laws, without overriding such requirements or laws); and

- x. management of personal data breaches and record-keeping obligation (with proposals to provide guidance on best practices for a data controller to effectively respond to the breaches, investigate and contain them, and implement measures to prevent the recurrence of similar breaches in the future).
- b. Personal Data Protection (Data Protection Officer) Regulations and Data Protection Officer Guideline (see [Public Consultation Paper No. 02/2024](#)), which seek to address:
- i. threshold requirement for mandatory appointment of DPO (with proposals for this requirement to apply only to a data controller or data processor who carries out data processing activities of a large scale, taking into account certain factors);
  - ii. consistency with other legal requirements for roles similar to a DPO (with proposals allowing the DPO to undertake additional job functions beyond data-specific roles);
  - iii. sector-specific risks for DPO when carrying out his functions (with proposals outlining the minimum responsibilities of the DPO);
  - iv. reporting line for DPO (with proposals requiring that the DPO has a direct reporting line or access to senior management team of the data controller or data processor, or to the personnel in an equivalent position);
  - v. regional appointment of DPO and local residency requirement (with proposals allowing a single DPO to serve multiple entities within the same group of companies for a data controller or data processor, and requiring the DPO to be ordinarily resident in Malaysia);
  - vi. minimum expertise and qualifications of DPO and certification requirements (with proposals for the appointed DPO to meet a prescribed minimum set of expertise and qualifications, and to complete the required training or certification programmes); and
  - vii. factors the Commissioner may consider in exercising discretion to mandate appointment of DPO (with proposals for the Commissioner to be empowered

to direct certain classes or specific data controller or data processor to appoint a DPO on a case-by-case basis, taking into account certain factors).

- c. Personal Data Protection (Right to Data Portability) Regulations and Data Portability Guidelines (see [Public Consultation Paper No. 03/2024](#)), which seek to address:
  - i. readiness for the right to data portability (with proposals for this requirement to apply when there is technical feasibility between the data controller and receiving data controller);
  - ii. types of personal data subject to the right to data portability (with proposals to limit the types of personal data to those directly provided by the data subject, processed based on consent (or explicit consent) or based on a contract to which the data subject is a party, processed by automated means, and excluding inferred or derived data);
  - iii. timeline for complying with a data portability request (with proposals to comply with the request within 21 days, with a possible extension of 14 days, similar to the timelines for data access and correction requests);
  - iv. historical data (with proposals that no time limit be imposed on data portability requests for personal data previously collected and retained by a data controller);
  - v. fees (with proposals allowing a data controller to charge a capped fee, similar to that for data access requests); and
  - vi. transmission of personal data arising from a data portability request (with proposals allowing a data controller to determine the best method for transmitting the requested data, provided that it complies with any common standards or formats specified by the Commissioner or relevant data controller forum, or that there are appropriate security measures to ensure the data is securely transmitted to the correct destination or receiving data controller).
- d. Updated Personal Data Protection Standards (“**Standards**”) (see [Public Consultation Paper No. 04/2024](#)), which seek to:

- i. replace the prescriptive “black and white” rules in the Standards with “outcome-based” requirements;
  - ii. replace the specific security standards for electronically and non-electronically processed personal data, respectively, with general security standards which are applicable to both;
  - iii. expand the retention standards to cover the retention period, documentation and records for the retention and disposal of personal data, methods for destruction or deletion of personal data and third-party retention of personal data;
  - iv. expand the data integrity standards to include measures for data validation and verification, data quality monitoring, data consistency and data lifecycle management; and
  - v. recognize industry certifications as a means for a data controller or data processor to demonstrate compliance with the Standards (for instance, ISO 27001 certification for information security management system, ISO 27017 certification on information security controls for the provision and use of cloud services, and ISO 27701 certification for privacy information management system).
- e. Cross-Border Personal Data Transfer Guidelines (see [Public Consultation Paper No. 05/2024](#)), which seek to address the following, including the prescribed conditions for transferring personal data to a place outside Malaysia (“**that place**”):
- i. new conditions that there is in that place in force any law which is substantially similar to the PDPA, or that place ensures an adequate level of protection in relation to the processing of personal data which is at least equivalent to the level of protection afforded by the PDPA (with proposals requiring a data controller to conduct a transfer impact assessment to determine whether that place has such a law or protection level);
  - ii. consent as the basis for the transfer (with proposals requiring a data controller to notify data subjects in writing about the cross-border data transfer and to obtain their consent);

- iii. necessity for performance of contract or protection of vital interests of data subjects as the basis for the transfer (with proposals requiring a data controller to consider certain factors to determine whether the transfer is necessary for these purposes);
- iv. use of binding corporate rules (with proposals to recognize this as proof that the data controller has taken all reasonable precautions and exercised all due diligence to justify the transfer);
- v. use of standard contractual clauses (with proposals to recognize this as proof that the data controller has taken all reasonable precautions and exercised all due diligence to justify the transfer);
- vi. use of certification mechanism (with proposals to recognize this as proof that the data controller has taken all reasonable precautions and exercised all due diligence to justify the transfer); and
- vii. record-keeping obligation (with proposals requiring a data controller to keep and maintain relevant records that sufficiently demonstrate that the transfer complies with the applicable condition(s) under the PDPA).

### **Next steps**

The Amendment Act marks a pivotal step forward in strengthening Malaysia's data protection framework, aligning it more closely with global practices and international standards. These amendments ensure that personal data protection remains a central priority in an increasingly digital world. With the Amendment Act coming into force, it is essential for organizations to proactively familiarize themselves with the new obligations and take necessary steps to adequately prepare for the upcoming amendments. These include:

- a. reviewing and updating internal data protection policies, practices and procedures to align them with the new requirements;
- b. developing a data breach crisis plan that establishes clear protocols for addressing personal data protection breaches; and
- c. revisiting contracts with third-party data processors to ensure they include appropriate indemnities and warranties to safeguard the organization in the event of a data breach.

This approach will not only ensure compliance with the amended PDPA, but also foster a robust culture of privacy and accountability within the organization. By embracing these changes, businesses can better safeguard individuals' personal data, mitigate potential risks and enhance their reputation as responsible stewards of privacy in a rapidly evolving digital landscape.

*This article is authored by our Partner, Ms Lee Lin Li and Senior Associate, Ms Chong Kah Yee. The information in this article is intended only for general information and is not a legal opinion or professional advice.*

**Written by:****LEE LIN LI**

Partner

[linli.lee@taypartners.com.my](mailto:linli.lee@taypartners.com.my)**CHONG KAH YEE**

Senior Associate

[kahyee.chong@taypartners.com.my](mailto:kahyee.chong@taypartners.com.my)