A. Introduction

The Malaysian Personal Data Protection (Amendment) Act 2024 ("**Amendment Act**") introduces significant changes to Malaysia's data protection framework under the Personal Data Protection Act 2010 ("**PDPA**"). The Amendment Act is enacted to address emerging challenges in data privacy, cybersecurity, and cross-border data transfers and aligning it with the European Union's General Data Protection Regulation ("**GDPR**"). The Amendment Act will come into operation in three stages (i.e. on 1 January 2025, 1 April 2025 and 1 June 2025). This article examines the key provisions of the Amendment Act, its implications for businesses and individuals, and the practical steps required for compliance.

B. Key Amendments Introduced by the Amendment Act

1. Expanded Scope of Personal Data

The Amendment Act broadens the definition of "sensitive personal data" to include biometric data[1]. **The term "biometric data" means any personal data resulting from technical processing relating to the physical, physiological or behavioural characteristics of a person.** This encompasses, though is not restricted to, data utilised for facial recognition, fingerprint authentication, voice identification, retinal scanning, keystroke dynamics, eye-tracking, and the analysis of handwritten signatures. This expansion reflects the increasing digitisation of personal information and ensures that the law remains relevant in the face of technological advancements.

2. Replacing the term "Data Users" with "Data Controllers"

Replacing the term "Data User(s)" with "Data Controllers"[2] aligns the terminology with that of other data protection frameworks, such as the GDPR, creating consistency across regulatory jurisdiction.

3. Enhanced Data Processor Compliance

The current PDPA solely governs data controllers to comply with the Security Principle (i.e. taking practical steps to protect personal data from loss, misuse, modification, unauthorised or accidental access, or disclosure, alteration or destruction).[3] However, under the proposed amendments, data

[1] Section 3(b) and (c) of the Amendment Act (see Section 4 of the PDPA)
[2] Section 2 of the Amendment Act
[3] Section 9 of PDPA

processors will also be obligated to comply with the Security Principle.[4] This update aims to broaden data protection accountability to include data processors. Non-compliance with the PDPA provisions will now subject data processors to penalties under the PDPA as well.

4. **Data Breach Notification Obligations**

A significant addition to PDPA is the mandatory data breach notification requirement under Section 6 of the Amendment Act.[5] Data controllers are now obligated to notify the Personal Data Protection Commissioner ("**PDP Commissioner**") and affected data subjects in the event it causes or is likely to cause any "*significant harm*" to the data subject. This provision aims to enhance transparency and accountability in the event of cybersecurity incidents. To supplement this provision, the PDP Commissioner's Office released a guideline on data breach notifications, which should be reviewed in conjunction with the relevant circulars listed below:

(a) Personal Data Protection Guideline dated 25 February 2025 – Data Breach Notification (*Garis Panduan Perlindungan Data Peribadi DBN – Pemberitahuan Pelanggaran Data*)[6]
(b) e Circular of Personal Data Protection Commissioner No. 2/ 2025 (*Pekeliling Pesuruhjaya Perlindungan Data Peribadi Bilangan 2 Tahun 2025*) – in effect from 1 June 2025[7]

4.1. Definition of a "Significant Harm"

4.1.1. A personal data breach is considered to cause or is likely to cause "significant harm" if there is a risk that the compromised personal data[8]:

(a) may result in physical harm, financial loss, a negative effect on credit records or damage to or loss of property;
(b) may be misused for illegal purposes;
(c) consists of sensitive personal data;
(d) consists of personal data and other personal information which, when combined, could potentially enable identity fraud; or
(e) is of significant scale (if the number of affected data subjects exceed 1,000)[9]

4.2. Notification of Data Breach

4.2.1. Data Breach Notification to PDP Commissioner[10]:

(a) Within 72 hours of discovering a data breach, the data controller shall submit to the PDP Commissioner the following information:
(i) Details of the personal data breach
(ii) The potential consequences arising from the personal data breach;

---

[4] Section 5(a) of the Amendment Act (see Section 9 of the PDPA)
[5] Section 6 of the Amendment Act (see Section 12B of the PDPA)
[6] https://www.pdp.gov.my/ppdpv1/wp-content/uploads/2025/02/GARIS-PANDUAN-PERLINDUNGAN-DATA-PERIBADI_-PEMBERITAHUAN-PELANGGARAN-DATA-1.pdf dated 25 February 2025
[7] https://www.pdp.gov.my/ppdpv1/wp-content/uploads/2025/02/Pekeliling-DBN-1.pdf, effective on 1 June 2025
[8] Paragraph 5.2 of the Personal Data Protection Guideline dated 25 February 2025– Data Breach Notification: https://www.pdp.gov.my/ppdpv1/wp-content/uploads/2025/02/GARIS-PANDUAN-PERLINDUNGAN-DATA-PERIBADI_-PEMBERITAHUAN-PELANGGARAN-DATA-1.pdf dated 25 February 2025
[9] Paragraph 5.4 of the Personal Data Protection Guideline dated 25 February 2025– Data Breach Notification: https://www.pdp.gov.my/ppdpv1/wp-content/uploads/2025/02/GARIS-PANDUAN-PERLINDUNGAN-DATA-PERIBADI_-PEMBERITAHUAN-PELANGGARAN-DATA-1.pdf dated 25 February 2025
[10] Paragraph 7 of the Personal Data Protection Guideline dated 25 February 2025– Data Breach Notification: https://www.pdp.gov.my/ppdpv1/wp-content/uploads/2025/02/GARIS-PANDUAN-PERLINDUNGAN-DATA-PERIBADI_-PEMBERITAHUAN-PELANGGARAN-DATA-1.pdf dated 25 February 2025

(iii) The chronology of events leading to the loss of control over personal data;
(iv) Measures taken or proposed to be taken by the data controller to address the personal data breach, including steps implemented or planned to mitigate the possible adverse effects of the breach;
(v) Measures taken or proposed to be taken to address the affected data subjects; and
(vi) The contact details of the data protection officer or any other relevant contact person from whom further information on the personal data breach may be obtained.

(b) Notification to the PDP Commissioner shall be made through one of the following channels:
(i) completing the notification form available on the official website of the Department of Personal Data Protection (JPDP) at www.pdp.gov.my;
(ii) completing the notification form in Annex B and submitting it to the official e-mail address dbnpdp@pdp.gov.my; or
(iii) completing the notification form in Annex B and submitting a hard copy to the Commissioner.

4.2.2. Data Breach Notification to Affected Data Subjects:

(a) The notification to the affected data subjects must be made not later than seven (7) days after the initial data breach notification is made to the PDP Commissioner the following information:
(i) the details of the personal data breach that has occurred;
(ii) details on the potential consequences resulting from the personal data breach;
(iii) measures taken or proposed to be taken by the data controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects;
(iv) measures that the affected data subjects may take to eliminate or mitigate any potential adverse effects resulting from the data breach; and
(v) the contact details of the data protection officer or other contact point from whom more information regarding the personal data breach can be obtained

(b) Notification to the affected data subjects shall be individually through emails, SMS, direct messaging; and postal communication. However, in the event it is impracticable to do so, notification can be made by way of public communication amongst others notification on the official website, notice in printed media, social media posts and automated notification.

5. **Cross-Border Data Transfer Regulations**

The Amendment Act imposes stricter controls on cross-border data transfers. Any data controller transferring any personal data of a data subject to any place outside of Malaysia must ensure that the recipient country either has:[11]

(a) laws substantially similar to the PDPA; or
(b) an adequate level of protection equivalent to the PDPA.

6. **Increased Penalties for Non-Compliance**

To deter violations, the Amendment Act significantly increases the penalties for non-compliance. Organisations found guilty of breaching the PDPA may face fines of up to RM 1 million and / or up to three years of imprisonment (from up to RM300,000 and / or up to two years of imprisonment).[12]

Additionally, directors, managers, and other key officials of a data controller may face personal liability unless they can demonstrate that the offence was done without his/her knowledge, consent or connivance; and that he/her had taken all reasonable precautions and exercised due diligence to prevent the commission of the offence.[13]

7. **Introduction of Data Protection Officers (DPOs)**

The Amendment Act mandates the appointment of Data Protection Officers (DPOs)[14] for organisations that processes large volumes of personal data or engage in high-risk data processing activities. DPOs are responsible for ensuring compliance with the PDPA, advising on data protection impact assessments, and serving as the primary point of contact for data subjects and regulatory authorities.

To supplement this provision, the PDP Commissioner's Office released a guideline on DPOs which should be reviewed in conjunction with the relevant circulars listed below:

(a) Personal Data Protection Guideline dated 25 February 2025 - Appointment of Data Protection ("*Garis Panduan Perlindungan Data Peribadi – Pelantikan Pegawai Perlindungan Data*")[15].
(b) Circular of Personal Data Protection Commissioner No. 1/2025 (*Pekeliling Pesuruhjaya Perlindungan Data Peribadi Bilangan 1 Tahun* 2025) – in effect from 1 June 2025[16]

[11] Section 12 of the Amendment Act (see Section 129(2) of the PDPA)
[12] Section 4(b) of the Amendment Act (see Section 5(2) of the PDPA)
[13] Section 133 of the PDPA
[14] Section 6 of the Amendment Act (see Section 12A of the PDPA)
[15] https://www.pdp.gov.my/ppdpv1/wp-content/uploads/2025/02/GARIS-PANDUAN-PERLINDUNGAN-DATA-PERIBADI_PELANTIKAN-PEGAWAI-PERLINDUNGAN-DATA.pdf dated 25 February 2025
[16] https://www.pdp.gov.my/ppdpv1/wp-content/uploads/2025/02/Pekeliling-DPO.pdf, effective on 1 June 2025

7.1. Requirements for the appointment of a DPO[17]

7.1.1. A data controller and data processor are required to appoint one or more DPO if their processing of personal data involves:

(a) The personal data of over 20,000 data subjects;
(b) The sensitive personal data including financial information data exceeding 10,000 data subjects or
(c) Activities involving regular and systematic monitoring of personal data takes place.

7.2. The Expertise and Qualification of a DPO[18]

7.2.1. There are no minimum professional qualifications required of the DPO. However, the data controller and data processor must ensure that the DPOs can demonstrate a sound level of the following skills, qualities and expertise:

(a) knowledge of the PDPA laws (including any other applicable data protection laws, where relevant);
(b) understand the data controller or data processor's business operations and the personal data processing operations that carried out;
(c) understanding of information technology and data security;
(d) personal qualities such as integrity, understanding of corporate governance and high professional ethics;
(e) ability to promote data protection culture within the organisation;

7.2.2. A DPO may be an internally or externally appointed for a term of no less than two years.

7.2.3. The appointed DPO must be ordinarily resident in Malaysia (i.e. physically in Malaysia for at least 180 days a year) and proficient in Bahasa Melayu and English languages.

7.2.4. A DPO may be a part-time or full-time position and may perform additional tasks as part of his job scope, provided there is no conflict of interest. Such personnel could be a legal counsel, a compliance officer, or a risk manager with direct reporting access to senior management.

8. Rights to data portability

Section 43A[19] establishes a new right to data portability, granting data subjects the authority to request the transfer of their personal data between different data controllers.

C. Implications for Businesses

The implementation of the Amendment Act requires businesses to undertake a comprehensive review of their data protection practices. Key steps include:

---

[17] Paragraph 4.2 of the Personal Data Protection Guideline dated 25 February 2025 - Appointment of Data Protection: https://www.pdp.gov.my/ppdpv1/wp-content/uploads/2025/02/GARIS-PANDUAN-PERLINDUNGAN-DATA-PERIBADI_PELANTIKAN-PEGAWAI-PERLINDUNGAN-DATA.pdf dated 25 February 2025

[18] Paragraph 5 and 6 of the Personal Data Protection Guideline dated 25 February 2025 - Appointment of Data Protection: https://www.pdp.gov.my/ppdpv1/wp-content/uploads/2025/02/GARIS-PANDUAN-PERLINDUNGAN-DATA-PERIBADI_PELANTIKAN-PEGAWAI-PERLINDUNGAN-DATA.pdf dated 25 February 2025

[19] Section 9 of the Amendment Act (see Section 43A of the PDPA)

1. **Updating Privacy Policies**: Businesses must revise their privacy policies to reflect enhanced consent requirements in relation to processing of biometric data and provide clear information about data processing activities. Businesses are required to adopt the wording “Data Controllers” from its predecessor “Data Users”.

2. **Strengthening security policy and constantly audit data practices**: Business are required to actively review their data practices, establish strong protective measures, safeguards and ensure full compliance with the principles under the PDPA. This is more pertinent since Data Processors are required to comply with the Security Principle.

3. **Appointment of a DPO**: Businesses will need to formalise and update their internal data protection policies, ensuring that the role of the Data Protection Officer (DPO) is well-defined and integrated into their operational structure. This may require organisational changes and additional staffing.

4. **Implementing Data Breach Response Plans**: Organisations need to establish robust incident response mechanisms to comply with the 72-hour notification requirement to notify the PDP Commissioner and seven (7) days notification period to notify the affected data subjects should there be a data breach.

5. **Procedure of Data Portability**: The introduction of new rights, such as data portability, empowers individuals to request the transfer of their personal data between service providers. Businesses must establish processes to handle such requests efficiently, which may involve technological upgrades and procedural changes.

6. **Conducting a Data Protection Impact Assessments (DPIAs)**: Although a DPIA is required under the GDPR[20] and not PDPA, the GDPR applies to businesses and companies within and outside the EU (which may include Malaysia)[21]. DPIA is crucial as it understands and addresses potential high risk data processing (such as bio-metrics) and to later mitigate the identified risks to data subjects.

7. **Training Employees:** Staff must be trained on the new requirements to ensure compliance and foster a culture of data protection within the organisation.

D. Conclusion

The Malaysian Personal Data Protection (Amendment) Act 2024 marks a significant step forward in strengthening the country's data protection regime. By aligning with international standards and addressing contemporary challenges, the Amendment Act enhances the rights of individuals and imposes greater responsibilities on organisations. Businesses must act proactively to ensure compliance, while individuals can expect greater protection and control over their personal data. As Malaysia continues to navigate the complexities of the digital economy, the Amendment Act provides a robust framework for safeguarding personal data in an increasingly interconnected world.

[20] Article 35 of the GDPR
[21] Article 3 of the GDPR

Further information

Should you have any questions on the implications of this Act or how this development may affect you or your business, please get in touch with the following person:

Chuck Siew Ka Wai

Partner

kwsiew@tsl-legal.com

Kok Hao Ying

Senior Associate

hykok@tsl-legal.com