ASL
Adnan Sundra & Low

NAVIGATING THE NEW ERA OF DATA PRIVACY: COMPLIANCE BLUEPRINT FOR NAVIGATING MALAYSIA'S PDP (AMENDMENT) ACT 2024

MONTH :
March 2025

BY :
Sri Sarguna Raj,
Steven Cheok Hou Cher
& Nicole Chong

NAVIGATING THE NEW ERA OF DATA PRIVACY: COMPLIANCE BLUEPRINT FOR NAVIGATING MALAYSIA'S PDP (AMENDMENT) ACT 2024

Introduction

The Personal Data Protection Act 2010 ("**PDPA**") in Malaysia is undergoing a seismic shift with the introduction of the PDP (Amendment) Act 2024 ("**the Amendment Act**"). Businesses now face stricter regulations and higher stakes in managing personal data. Therefore, compliance is not merely an option—it is a necessity.

Previously, we published an article on the Proposed Amendments in the Personal Data Protection (Amendment) Bill 2024, which outlines the amendments proposed by the Amendment Bill and has officially come into effect in 2025. In line with the above, this article explores the critical updates under the Amendment Act, detailing specific actions businesses must take to ensure compliance. Organisations can minimise risks and optimise their data protection frameworks by taking the proper steps.

The Stakes Are Higher—Here's What's Changing

In 2024, the Malaysian government's updates to the PDPA elevate data protection standards across three critical areas: **data subject rights, accountability for data controllers** and **processors, and tighter consent protocols**. Here is what you need to know:

Effective 1 April 2025:

1. Substitution of the term "data users" with "data controllers";
2. Inclusion of "biometric data" as a category of sensitive personal data;
3. Introduction of increased penalties for violations of the Personal Data Protection Principles;
4. Expansion of the Security Principle to include data processors;
5. Elimination of the whitelisting framework for cross-border data transfers;

Effective 1 June 2025:

6. Implementation of a new requirement of appointing data protection officer for both data controllers and data

processors;

7. Establishment of a mandatory personal data breach notification system for data controllers, mandating data breach reporting to both the Personal Data Protection Commissioner ("the Commissioner") and the affected data subjects;

8. Grant data subjects a new "right to data portability".

Key Details:

1. **Substitution of the Term "Data Users" With "Data Controllers"**

   This nomenclature change streamlines the terminology used in other data protection regimes, such as the General Data Protection Regulation ("**GDPR**") in the European Union.

   Key Measures for Businesses: While there is no significant effect from a legal perspective, businesses are required to adopt the wording of "Data Controllers" from its predecessor "Data User" in their data protection regimes e.g. privacy notices, policy and guidelines.

2. **Inclusion Of "Biometric Data" as a Category of Sensitive Personal Data**

The Amendment Act has expanded the definition of "*sensitive personal data*" to now include biometric data. Biometric data is defined as personal data derived from technical processing of an individual's physical, physiological, or behavioural characteristics. This includes, but is not limited to, information used for facial recognition, fingerprint verification, voice recognition, retinal scans, keystroke patterns, gaze tracking, and handwritten signature analysis.

Essentially, sensitive personal data is subject to stricter consent and security requirements under the PDPA due to its highly sensitive nature. Previously, the PDPA categorised sensitive personal data as information related to an individual's physical or mental health, political opinions, religious beliefs, or criminal offences. The inclusion of biometric data acknowledges the growing role of advanced technologies and artificial intelligence in processing such information, highlighting the need for enhanced protections.

Key Measures for Businesses:

Businesses that process biometric data must adopt measures to align with the heightened requirements for sensitive personal data under the amended PDPA, for example:

- **Updating Privacy Notices and Consent Mechanisms:** Revise privacy policies and consent clauses to ensure explicit and informed consent is obtained for the processing of biometric data.
- **Strengthening Security Protocols:** Implement robust operational measures safeguarding biometric data and the processing of biometric data against risks such as unauthorised access, misuse, or breaches.

3. Introduction of Increased Penalties for Violations of The Personal Data Protection Principles ("the Principles")

The Amendment Act introduces significantly higher penalties for non-compliance with the 7 Principles, which are the cornerstone of responsible personal data management. These principles encompass general, notice and choice, disclosure, security, retention, data integrity, and access requirements. Under the revised framework, penalties have been raised from the previous maximum of RM 300,000 in fines and/or two years of imprisonment to a new ceiling of RM 1,000,000 in fines and/or three years of imprisonment.

Additionally, directors, managers and other key officers of a data controller may face individual liability unless they can demonstrate that the offence occurred without their knowledge and that reasonable precautions and due diligence were exercised to prevent it.

Key Measures for Businesses: To proactively audit their data practices, implement robust safeguards, and ensure comprehensive adherence to the principles stipulated above.

4. Expansion of the Security Principle to Include Data Processors

The Amendment Act imposes direct legal obligations on data processors, marking a departure from the previous framework where compliance was primarily the responsibility of data controllers. With this amendment, data

processors are now directly required to comply with the Security Principle under section 9 of the PDPA. This principle mandates data processors to take practical steps to protect personal data from loss, misuse, unauthorised access, modification, or destruction.

Failure to meet these requirements may result in penalties of up to RM 1,000,000 in fines and/or imprisonment for up to 3 years under the enhanced enforcement framework.

Key Measures for Businesses:

- **Develop and maintain a comprehensive security policy** that aligns with the standards prescribed by the Personal Data Protection Standard 2015 and the Personal Data Protection Regulations 2013.
- **Conduct regular audits** to ensure compliance with security measures and to identify and mitigate vulnerabilities.
- **Implement robust technical and organizational safeguards** such as encryption, access controls, and monitoring systems, to prevent data breaches.

5. Implementation of a New Requirement of Appointing Data Protection Officers ("DPO") for both Data Controllers and Data Processors

On 25 February 2025, the Personal Data Protection Commissioner Office ("**the Commissioner Office**") published the following data protection guideline to be read in conjunction with the following:

- Personal Data Protection Guideline - Appointment of Data Protection Officer
- The Circular of Personal Data Protection Commissioner No. 1/2025 (Appointment of Data Protection Officer)

5.1 Criteria for Mandatory DPO Appointment

By virtue of the insertion of section 12A, the data controller or data processor must now appoint a DPO where their processing of personal data involves:

- The personal data of over 20,000 data subjects;

- The sensitive personal data (e.g. financial information) of over 10,000 data subject; or
- Regular and systematic monitoring of personal data takes place. Non-exhaustive examples of such activities include:

  a) Any form of activity where data subjects are tracked and profiled online or offline for purposes of behavioural advertising

  b) A retail website that uses algorithms to monitor the searches and purchases of its users and, based on this information, offers recommendations to them. Notably, the management of a loyalty programme may not fall within this category, where the purpose of regular and systematic monitoring of the data subjects is to manage their accounts and not to monitor their purchase behaviours.

5.2 Appointment Requirements:

The guidelines and circular have elaborated the conditions under which a DPO may be appointed as provided below:

a) A DPO may be an internally or externally appointed for a term of no less than 2 years.

b) 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.

c) There are no minimum professional qualifications required of the DPO. However, the DPOs are expected to demonstrate knowledge of the PDPA laws as well as an understanding of business operations, personal data processing operations, and information technology & data security.

d) The Commissioner may decide on courses and training programmes for DPOs to attend.

e) 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.

5.3 Notification to the Commissioner upon the Appointment of DPO

a) Upon the appointment of a data officer, the data controller shall register the appointed DPO and submit their business contact information within 21 days from the date of appointment. The registration and submission can be done via https://daftar.pdp.gov.my/. The data controller and data processor shall create a designated official email for the DPO separate from the business work email and publish the contact information of the DPO through the following:

- Official website and other official media, including social media platforms and intranet;
- Personal data protection notices;
- Security policies and guidelines.

b) Where the data controller does not fulfil the mandatory appointment criteria as but still wishes to appoint a DPO on his own initiative, there is no express requirement to register. Nevertheless, it would be good practice to do so.

c) Where there is a change of information relating to the DPO e.g. change in DPO or business contact information of the DPO, the data controller must update the changes within 14 days from the effective date of the new appointment.

5.4 Core Responsibilities of a DPO

Responsibilities to the Data Controller or Data Processor	Responsibilities to the Commissioner	Responsibilities to the Data Subjects
➢ inform and provide advice to the data controller or data processor on the processing of personal data; and ➢ support the data controller or data processor in complying with the PDPA laws and staying informed of data processing risks	As the liaison officer and main point of contact between the data controller or data processor and the Commissioner, the DPO's duties are: ➢ facilitate access to documents and information during inspections/investigations conducted by the Commissioner; ➢ prepare and submit information required by the Commissioner on any personal data breaches; and ➢ represent the data controller or data processor in industry engagement sessions or programmes organised by the Commissioner.	As the facilitator and contact person on behalf of the data controller or data processor, the DPO's duties to the data subjects are: ➢ handle issues related to the processing of personal data including personal data breaches; ➢ manage requests concerning the exercise of the data subject's rights; and ➢ educate data subjects about the processing of their personal data.

5.5 Key Measures for Businesses

While having a dedicated person to ensure that the protection of data can be upheld at the highest standard, the appointment of a DPO does not discharge the data controller and data processor of their obligations under the PDPA 2010.

Businesses are to proactively review and formalise internal data protection policies, ensuring the DPO's role is well-defined and integrated into their operational structure. This includes equipping DPOs with the authority and resources necessary to oversee compliance effectively. Organisations can further enhance their operations by conducting regular audits and investing in staff training on data protection best practices.

6. Elimination of the Whitelisting Framework for Cross-Border Data Transfers

Previously, the PDPA allowed the Minister to issue a whitelist of

countries where personal data could be transferred, based on the adequacy of their data protection laws. However, this system has been ineffective, as no countries have been added to the whitelist.

Under the amended law, data controllers can now transfer personal data abroad under two conditions, as outlined in section 129(2) of the Amendment Act:

(i) The destination country's laws are substantially similar to the PDPA; or

(ii) The country ensures an adequate level of protection for personal data, equivalent to the PDPA's standards.

This shift places the responsibility on data controllers to assess the adequacy of foreign data protection laws. While this change provides greater flexibility, it may lead to practical challenges, especially for smaller organizations, as they will need to determine whether a country's data protection laws meet the necessary criteria.

Moreover, the Cross-Border Data Transfer Guidelines, which are currently being developed, will offer further clarity, including the possibility of adopting transfer mechanisms such as binding corporate rules or standard contractual clauses.

Key Measures for Businesses:

- **Evaluate Destination Jurisdictions:** Data controllers should review the data protection laws of countries they intend to transfer data to and assess their adequacy against Malaysian standards.
- **Prepare for Guidelines:** Stay updated on the Commissioner's Data Transfer Guidelines and align internal processes with any new mechanisms or standards introduced.
- **Document Compliance:** Implement robust documentation and due diligence procedures to support the legality of cross-border transfers and ensure transparency.

7. Establishment of a Mandatory Personal Data Breach Notification System for Data Controllers, Mandating Data Breach Reporting to Both the Commissioner and Affected Data Subjects

Section 12B provides for the mandatory data breach notification requirement for data controllers where there is a personal data breach. This section does not apply to data processors. Thus, the data controller is required to contractually impose a prompt notification obligation on his data processor concerning data breaches.

To complement this section, the Commissioner's Office had issued a data breach notification guideline, which is to be read together with the relevant circular as below:

- Personal Data Protection Guideline – Data Breach Notification ("**Data Breach Notification Guideline**")
- The Circular of Personal Data Protection Commissioner No. 2/2025 (Data Breach Notification)

7.1 Reporting Obligation on Personal Data Breach

Examples of a personal data breach — which broadly refers to any breach, loss, misuse, or unauthorized access of personal data are:

- An employee accidentally sending an email containing personal data to the wrong recipient.
- An employee leaving documents containing personal data on unattended desks or open areas.
- the alteration of personal data without permission.

Notably, not all breaches must be reported. Where there is a personal data breach likely to cause "*significant harm*" to the data subjects, the data controller must notify the Commissioner and the affected data subjects in the manner and form determined by the Commissioner without unnecessary delay. Here, a personal data breach is considered to cause or likely to cause "*significant harm*" if there is a risk that the compromised personal data:

(i) may result in physical harm, financial loss, a negative effect on credit;

(ii) records or damage to or loss of property;

(iii) may be misused for illegal purposes;

(iv) consists of sensitive personal data;

(v) consists of personal data and other personal information which, when

(vi) combined, could potentially enable identity fraud; or

(vii) is of significant scale e.g. affected data subjects exceed 1,000 individuals.

7.2 Reporting Mechanisms

a) Notification to the Commissioner

Upon the occurrence of the breach or confirmation upon investigation that a breach has occurred, the data controller or his DPO must notify the Commissioner as soon as practicable within 72 hours, through the following channels:

- completing the notification form available on the official website of the Department of Personal Data Protection (JPDP) at https://www.pdp.gov.my/;
- completing the notification form in Annex B (available in the Data Breach Notification Guideline) and submitting it to the official e-mail address dbnpdp@pdp.gov.my; or
- completing the notification form in Annex B and submitting a hard copy to the Commissioner.

b) Notification to the Data Subjects

Data subjects should be notified individually by way of email, SMS and so on. However, where it is impracticable to do so, notification can be done by way of public communication e.g. on official website/social media accounts, on

printed media and automated notifications.

7.3 Repercussions of Non-Compliance

Non-compliance with any obligations can result in penalties of up to RM250,000, imprisonment for up to 2 years, or both.

7.4 Key Measures for Businesses:

- **Develop a Data Breach Response Plan:** Establish clear procedures for identifying, managing, and reporting data breaches. This plan should outline the steps to take when a breach occurs, designate responsible personnel, and set timelines for internal and external notifications.
- **Conduct Periodic Training:** Educate employees about data protection principles, breach identification, and the importance of prompt reporting.
- **Review and Update Data Processing Agreements:** Ensure that contracts with data processors include clauses that mandate immediate notification of any data breaches and outline the responsibilities of each party in such events.
- **Implement Robust Security Measures:** Adopt advanced security technologies and practices to protect personal data from breaches. Regularly update systems, conduct vulnerability assessments, and monitor for potential threats.

8. Grant to Data Subjects a New "Right to Data Portability"

New section 43A introduces a new right to data portability, empowering data subjects to request the transfer of their personal data from one data controller to another. This right is subject to the following conditions:

- **Written or Electronic Request:** The data subject must submit the request in writing or via electronic means.
- **Technical Feasibility and Compatibility:** The transfer is contingent upon the technical feasibility and compatibility of the data format between the two data controllers.
- **Timely Transmission:** Once the request is received, the data controller must

complete the data transfer within a timeframe specified by the Commissioner.

Key Measures for Businesses

- **Assess Technical Infrastructure:** Evaluate existing systems to ensure they can handle data portability requests efficiently. This includes implementing compatible data formats and robust transfer protocols.
- **Update Privacy Notices and Data Subject Agreements:** Inform data subjects of their right to data portability and the process for submitting requests, ensuring transparency. Ensure that all data subject agreements (customer contracts, employee contracts, etc) reflect the new requirements.

Conclusion: Taking Proactive Actions to Safeguard Privacy and Mitigate Risk

The Amendment Act significantly alters the data protection landscape in Malaysia, placing greater responsibility on businesses to protect personal data and uphold individuals' rights. Ultimately, ensuring compliance with the Act is not just a regulatory obligation—it is an opportunity to enhance customer trust and demonstrate a commitment to data ethics. As the landscape of data privacy evolves globally, businesses in Malaysia must move swiftly to comply with the amendments, avoiding the risk of penalties while demonstrating their commitment to safeguarding privacy.

This article was written by our Intellectual Property, Media, Sports & Gaming partners, Sri Sarguna Raj, Steven Cheok Hou Cher & Nicole Chong, with the assistance of Soo An Qi, Lim Chaw Zen and Michelle Yap Siew Hui (Senior Associate, Associate & Pupil). It contains general information only. It does not constitute legal advice or an expression of legal opinion and should not be relied upon as such.