ORRADATA

Malaysia's Personal Data Protection Act (PDPA)

Simplified Explanation

A concise overview of principles, rights, and compliance requirements

www.orradata.com

Summary:

Malaysia's Personal Data Protection Act 2010 (PDPA) is a regulatory framework designed to protect the integrity and security of individuals' personal data in commercial transactions. Originally enforced in 2013 and significantly updated by the **Personal Data Protection (Amendment) Act 2024**, the law governs how private organizations (now termed "Data Controllers") collect, use, and process personal information based on seven core principles, including Notice and Choice, Security, and Data Integrity. The 2024 amendments modernized the Act to align closer with international standards like the GDPR, introducing mandatory data breach notifications, the appointment of Data Protection Officers (DPOs), the right to data portability, and stricter penalties for non-compliance, all aimed at boosting consumer confidence in the digital economy.

1. Overview & Scope

- The **PDPA 2010** regulates how **commercial organizations** (known as "data users" or—since 2024 amendments—**data controllers**) collect, use, and disclose **personal data** in connection with commercial transactions in Malaysia
- It applies to organizations **based in Malaysia**, or those using equipment in Malaysia to process data—even if located abroad
- **Government agencies are exempt**, as public-sector entities are governed by separate data protocols

2. Key Definitions

- **Personal data**: Information relating directly or indirectly to an identifiable individual, including sensitive personal data and opinions about them
- **Sensitive Personal Data**: Includes details on physical/mental health, political or religious beliefs, criminal records—and since April 1, 2025—**biometric data** (e.g. fingerprints, facial recognition)
- **Data controller** (formerly "data user"): Entity that determines the purposes of processing.
- **Data processor**: Processes data on behalf of the controller. From April 2025, they have **direct legal obligations** under the Security Principle

3. Core Principles (Obligations)

Under Sections 6–12 of the Act, data controllers must follow these seven principles:

1. **General Principle**: Must have the data subject's consent before processing personal data; explicit consent is required for **sensitive personal data**

2. **Notice & Choice Principle**: Written notice must be provided (also in Malay or English) explaining data collection, purposes, rights, recipients, etc.—and offering a clear choice to consent
3. **Disclosure Principle**: Data may only be disclosed for stated purposes or to third parties listed in the notice—unless required by law or consented to otherwise
4. **Security Principle**: Take practical measures (based on the PDPC's Security Standard 2015) to prevent loss, misuse, unauthorized access, alteration, or destruction of data
5. **Retention Principle**: Do not retain data longer than necessary. Destroy it securely once it's no longer needed for stated purposes
6. **Data Integrity Principle**: Ensure data remains accurate, complete, and current—especially where it's used or disclosed
7. **Access Principle**: Allow data subjects to request access to (and correction of) their personal data, particularly when it's inaccurate or outdated

4. Subsidiary Legislation and Standards

Organizations must also comply with:

- **PDPA Regulations (2013)**, including data-user registration requirements and fees.
- **PDPA Standard 2015**, covering minimum standards for security, retention, and data integrity.
- **Codes of Practice** for specific industries (e.g. banking, communications, utilities, insurance, aviation) issued by the PDPC

5. Registration Requirement

Certain sectors must **register** with the PDPC, such as communications, banking, insurance, health, education, real estate, services, utilities, tourism, direct selling, transport, pawnbrokers, and moneylenders

- Failure to register and process data is punishable by up to **RM 500,000 fine or 3 years imprisonment**, or both

6. 2024–2025 Key Amendments

Major changes as of **April–June 2025** include

- **Terminology shift**: "Data user" becomes **"data controller"**, aligning terminology with global norms
- **Data processors** now directly subject to the **Security Principle**, with penalties if they fail to comply (fines up to RM 1 M or 3 years imprisonment)
- **Mandatory Data Protection Officer (DPO)** appointment by June 1, 2025 for controllers and processors. DPOs must be registered, resident in Malaysia, and accountable for PDPA compliance
- **Mandatory Breach Notification**:
    - Controllers must notify the Commissioner **"as soon as practicable"** after a breach.
    - And notify data subjects **without undue delay** if there is significant harm risk

- **Introduction of Data Portability**: Individuals can request transfer of their data to another controller where technically feasible
- **Definition expanded**: Biometric data is now categorized as **sensitive personal data** requiring explicit consent. Also, data of deceased individuals is **excluded** from PDPA scope
- **Increased penalties**: Breaches of the seven PDPA principles now attract fines up to **RM 1 million** and/or imprisonment up to **3 years** (up from RM 300K / 2 years)

7. Powers & Penalties

- Violating core principles may lead to:
  - Up to **RM 1 million fine** or **3 years imprisonment**, or both.
  - Company directors/officers can also be held personally liable
- Unregistered required controllers: **RM 500K fine** and/or **3 years prison** for operating without registration

8. At-a-Glance Summary

Area	Key Requirement
Scope	Covers commercial data controllers/processors in Malaysia
Consent & Notice	Written notice; consent required (explicit for sensitive/biometric data)
Use & Disclosure	Only for notified purposes; third-party disclosure restricted
Security	Practical safeguards per PDPC standards
Retention	No longer than needed; secure disposal required
Accuracy	Keep data accurate and up to date
Access & Correction	Right to review and correct own data
Registration	Mandatory for certain sectors
Processor Obligations	Direct responsibility for security from April 2025
DPO Appointment	Mandatory by June 1, 2025 for controllers & processors
Breach Notification	Notify Commissioner ASAP; notify individuals if significant harm
Data Portability	New right to request data transfer to another controller
Penalties	Fines up to RM 1 M, imprisonment up to 3 years; registrant sanctions for non-registration