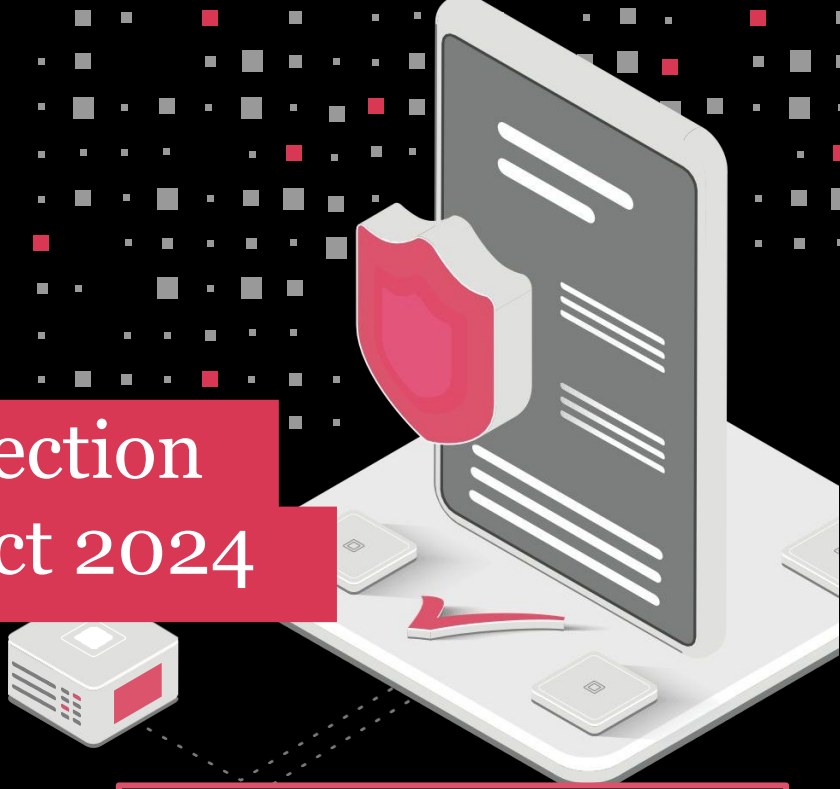
Personal Data Protection (Amendment) Act 2024



The Personal Data Protection Act 2010 (PDPA) has been the main form of legislation that regulates the processing of personal data in commercial transactions in Malaysia.

The Personal Data Protection (Amendment) Act 2024 amends the PDPA to be more closely aligned with the international standards for data protection.

Key amendments include:

- Data processors face new obligations under the Act
- The term “data controller” replaces "data user" to enhance clarity and improve alignment with international standards
- It is now mandatory to appoint a data protection officer(s)
- Data controllers must inform authorities and affected individuals in case of a data breach

Timeline of changes

- **2010:** PDPA enacted to regulate personal data in commercial transactions
- **2013:** PDPA came into force
- **2020:** The public consultation paper identified 22 proposed improvements to PDPA
- **2022:** Minister indicated certain amendments to the PDPA was due to be tabled in the Parliament, but was put on hold
- **July 2024:** The proposed PDPA amendments were approved by Cabinet, and subsequently passed in both Dewan Rakyat and Dewan Negara
- **Oct 2024:** Personal Data Protection (Amendment) Act 2024 received the royal assent and has been published in the Federal Gazette

Key concepts

Data controller

In the 2024 Act, the term “data controller” replaces "data user". This refers to those who processes any personal data or has control over or authorises the processing of any personal data.

Data processor

This refers to those who processes personal data on behalf of data controller. Data processors are now obliged to take steps to protect personal data from loss, misuse, unauthorised access and other risks.

Data protection officer (DPO)

Data controllers and data processors must designate a DPO. The DPO will be accountable to the data controller and data processor for ensuring the organisation's adherence to the PDPA.

Mandatory data breach notification

Data controllers must promptly notify the PDP Commissioner of any data breach, or face a fine of up to RM250,000 and/or up to two years in prison.

Biometric data

"Biometric data" has been added to the 2024 Act and is now classified as sensitive personal data, which requires more stringent handling procedures.

Data portability rights

Individuals can now request their data to be transferred to another service which facilitates easier switching between service providers.

Data transfer abroad

Data can be transferred to countries with adequate protection laws. This facilitates the protection of international data transfers

PDPA Act 2024

The proposed amendments in the 2024 Act are expected to align Malaysian data protection laws more closely with international standards.

Highlighted below are the salient amendments proposed in the Act.

Feature	PDPA 2010	2024 Act
Terminology for data user	Originally referred to as "**Data user**"	Changed to **"Data controller"**
Cross border data transfer	Transfers out to whitelisted countries were allowed with data subject's consent or for contract necessity. Although no countries were ultimately officially whitelisted	Whitelist regime for cross border data transfer were removed. Transfers are allowed to countries with similar data protection laws, or adequate protections; exceptions still apply
Penalties for breach of personal data protection principles	Penalties up to RM300,000 and/or two years of imprisonment	Increased penalties up to RM1 million and/or three years of imprisonment
Biometric data as sensitive personal data	Not specifically addressed	Considered sensitive; defined as data from technical processing of physical, physiological or behavioural traits
Data subject's right to data portability	No provision for data portability	Right granted, subject to technical feasibility and data format compatibility
Mandatory personal data breach notification	No requirement for breach notification	Required to notify the PDP Commissioner as well as affected individuals if the breach causes or is likely to cause significant harm to the individuals
Obligations on data processors	Data processors are not directly obligated	Data processors must adhere to security requirements and are subject to penalties for breaches
Mandatory appointment of a data protection officer (DPO)	Requirement did not exist	New mandatory requirement to appoint a DPO

Key privacy risks and actions for CDOs and CPOs

For Chief Data Officers (CDOs) and Chief Privacy Officers (CPOs) or equivalent

In the evolving digital environment, CDOs and CPOs face critical data privacy challenges. To mitigate risks and ensure regulatory compliance, consider the following actions:

Update privacy frameworks

Align data privacy policies with the latest PDPA regulations. Appoint a DPO to oversee compliance, coordinate with the PDP Commissioner, and manage regular audits

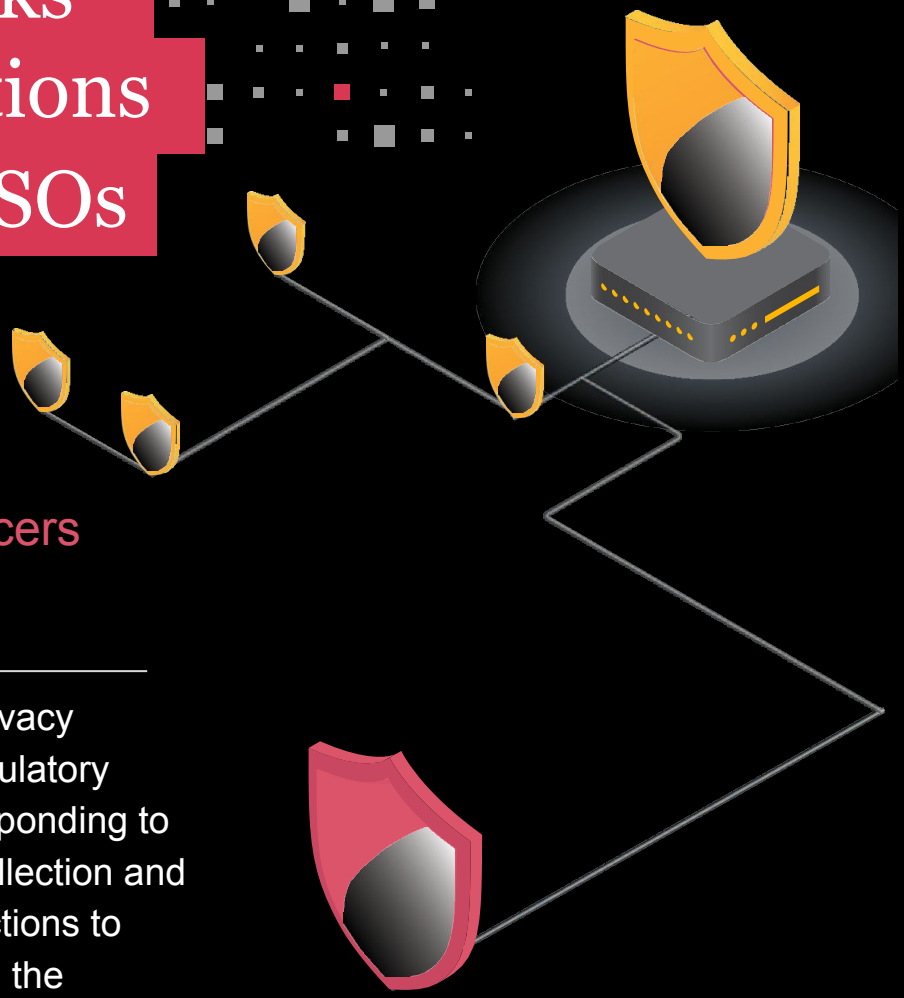
Standardise procedures for data portability

Develop standardised procedures for handling data portability requests, including secure identity verification and data transmission. Update privacy policies to communicate these rights to customers

Ensure compliance with cross-border data transfer requirements

Assess data protection laws in receiving countries and implement Standard Contractual Clauses (SCCs). Regularly review and update policies to ensure compliance with cross-border data regulations

Key privacy risks and actions for CIOs or CISOs



For Chief Information Officers (CIOs), Chief Information Security Officers (CISOs) or equivalent

For CIO and CISO, key data privacy concerns focus on ensuring regulatory compliance, preventing and responding to breaches, and securing data collection and processing practices. Critical actions to address these concerns include the following:

Establish a comprehensive data protection program

Establish a comprehensive data protection program by understanding the data lifecycle, and implementing policies, procedures, and technologies - such as Privacy Enhancement Technologies (PETs) - to safeguard personal data from unauthorised access, breaches, and evolving security threats.

Enhance incident response

Establish detailed procedures for detecting, assessing, and reporting data breaches. Invest in automated detection and real-time monitoring technologies to swiftly address potential data breaches and reporting obligations.

Key privacy risks and actions for Compliance and Audit

For Compliance and Internal Audit teams

Compliance and Internal Audit are key governance mechanisms for ensuring data privacy measures comply with the latest regulations and align with company goals. Key actions to develop an effective compliance and audit plan include the following:

Understand data privacy obligations

Collaborate with data privacy stakeholders to understand privacy obligations and mitigation strategies. Integrate data privacy risks and compliance requirements into the internal audit risk assessment and compliance gap analysis process.

Develop risk-based audit plans and compliance program for data privacy

Create audit plans that address data privacy practices, including collection, processing and transfer, to ensure ongoing compliance with PDPA guidelines. Employ new methodologies that integrate governance and technology aspects to assess the effectiveness of privacy controls.

“

Compliance with the PDPA isn't solely the responsibility of legal, compliance, or security teams, it's a collective obligation. Everyone in the organisation must understand their role in safeguarding personal data.

The 2024 Act is timely. It provides much-needed clarity to enhance the country’s data protection framework, level the playing field and positions Malaysia as a competitive and attractive destination in the global market.

Now is the time to rethink your data governance framework, assess your third-party risks, and accelerate efficiencies through standardisation and automation to secure the way you collect, process and transfer personal data.

”

Clarence Chan
Digital Trust and Cybersecurity Leader, PwC Malaysia
+60 (12) 712 1285
clarence.ck.chan@pwc.com

Glenda Eng
Director, Risk Services, PwC Malaysia
+60 (12) 692 0590
glenda.hs.eng@pwc.com