Wong & Partners.
Member Firm of
Baker & McKenzie International

Client Alert

May 2026

Malaysia: New Personal Data Protection Guidelines

In brief

Following a public consultation in 2025, Malaysia's Personal Data Protection Commissioner (PDPC) has issued the following new guidelines:

- Data Protection Impact Assessment (DPIA)
- Data Protection by Design (DPbD)
- Automated Decision-Making and Profiling (ADMP)

This client alert provides a summary of these three guidelines and key takeaways for organizations subject to Malaysia's Personal Data Protection Act 2010 (PDPA).

Contents

Click any heading above to jump straight to that section.

DPIA Guideline

The concept of DPIA stems from one of the responsibilities of a Data Protection Officer (DPO) under Circular PDPC No. 1/2025 i.e., to provide support and advice regarding the implementation of DPIA in accordance with such requirements as may be determined by PDPC from time to time and monitor compliance.

Such requirements, as set out in the DPIA Guideline, are summarized as follows:

❖ What is a DPIA?

A DPIA is essentially a process to analyze and mitigate personal data protection risks of a planned processing operation. It involves identifying, assessing, and managing such risks based on the organization's functions, requirements, and processes.

❖ Who is responsible for carrying out a DPIA?

Data controllers, specifically their senior management, bear the ultimate responsibility. Their respective DPO is required to develop customized DPIA template or checklist, identify whether a DPIA needs to be carried out, and provide advice on the implementation of DPIA and risk mitigation measures.

❖ When must a DPIA be carried out?

When a processing operation is likely to result in a high risk to the protection of personal data for the data subject, as follows:

- Where it is deemed likely to result in high risk (using quantitative thresholds) – processing sensitive personal data[1] (including financial information data) involving more than 10,000 data subjects, or other personal data involving more than 20,000 data subjects.

[1] Under the PDPA, "sensitive personal data" is essentially personal data relating to (a) physical or mental health or condition; (b) political opinions; (c) religious or similar beliefs; (d) commission or alleged commission of offence; or (e) biometric data.

- Based on the DPO's best judgment (based on qualitative factors) – e.g., potential legal or significant effects on the data subject, systematic monitoring of the data subject, use of innovative technologies, targeting of children or vulnerable individuals.

The goal is to ensure that data protection is a key focal point of risk assessment before an organization embarks on personal data processing.

❖ How to carry out a DPIA?

This involves the following five steps (a suggested template is provided in the DPIA Guideline):

- Describe the processing operation, including its nature, scope, context and the purposes.
- Evaluate the compliance, necessity, and proportionality of the processing operation.
- Identify and analyze the specific risks to the protection of personal data of the data subject.
- Consider measures to be taken to address the specific risks identified.
- Assess the overall residual risk level of the processing operation.

❖ What to do after carrying out a DPIA?

- Report to senior management for input on whether and how to proceed with the processing operation.
- Implement the identified risk mitigation measures.
- Carry out a refreshed DPIA, when the two-year validity period expires.
- Keep the relevant records for at least two years from the cessation of the processing operation, which shall be made available for inspection upon the PDPC's request.

DPbD Guideline

DPbD is centered around implementing the existing seven Personal Data Protection Principles under the PDPA. It involves **incorporating appropriate technical and organizational measures** into the **entire lifecycle** of a data processing activity.

For each of the Personal Data Protection Principles, the DPbD Guideline introduces non-prescriptive and non-exhaustive concepts, applications and checklists, which organizations may adapt based on their personal data processing operations and specific risk profile. These are mainly underpinned by the following DPbD elements:

Proactiveness	End-to-end protection	Transparency	User-centricity
• Anticipating and preventing risks before they occur, by establishing governance and resources and by designing systems that minimise data use and protect personal data by default.	• Ensuring the entire lifecycle of the personal data involved, including collection, processing, storage and disposal, comply with the Personal Data Protection Principles.	• Demonstrating accountability, by being open and honest about how personal data is handled and be prepared to demonstrate compliance with the stated practices.	• Recognising that personal data ultimately belongs to the data subjects and giving them control, by conciously designing projects, products, services, systems and processes around their interests and needs.

Further, the DPbD Guideline also provides that DPbD is about establishing a **culture that adopts a principled and proactive approach to personal data management,** which shall be applied across the organization and reflected in its products, services, governance and operations. To this end, it shall involve the following:

- Clear commitment from senior management to set and enforce high standards.
- Fostering a culture where all stakeholders share a commitment to continuous improvement in data protection standards.
- Establishing processes to identify gaps in current designs and practices and address issues before they occur proactively and systematically.

ADMP Guideline

ADMP involves two separate but related concepts:

Automated decision-making (ADM)

This means the process of making decisions without human involvement (including where human influence is minimal e.g., human merely inputs the data to be processed) using wholly or partly automated means.

Profiling

This means any form of automated processing of personal data to evaluate certain personal aspects relating to a data subject, in particular to analyse or predict aspects concerning that data subject.

Before carrying out any ADM or profiling, a **DPIA must first be carried out** in accordance with the aforementioned DPIA Guideline.

Further, if an ADMP may result in legal effects concerning the data subject (e.g., contract termination) or significantly affect the data subject (e.g., prolonged impact), the following **requirements** apply to the data controller:

- Ensure compliance with the PDPA (e.g., Section 40 on explicit consent or another exception for processing sensitive personal data) in order to process for ADMP.
- Inform data subjects about the ADMP processing in accordance with Section 7 of the PDPA by written notice, which shall be easily accessible and updated quickly as the ADMP activities evolve.
- Ensure accessible, straightforward, user-friendly mechanisms and processes are established for data subjects to exercise their right under Section 38 of the PDPA to withdraw consent.
- Inform data subjects of their right to withdraw consent, including the mechanisms and processes available for exercising such right.

Key takeaways

These developments are reflective of the increasing maturity of the personal data protection landscape in Malaysia, and signals how protection of personal data can become a key market differentiator for an organization. If not already done therefore:

❖ Organizations should promptly seek to **build in the need for DPIAs** within their data processing and governance frameworks especially with respect to high risk personal data processing.
❖ Organizations, presently undertaking ADM and profiling activities (or will shortly embark on these initiatives), should also **take note of the additional requirements to be complied with** (which may require changes not just to personal data protection notices but also to workflows and customer/user journeys).
❖ Organizations, at any stage of their data processing and governance initiatives, may wish to **work together with a multi-stakeholder team** (e.g., product design, business, data security and IT teams) to start **taking into account the DPbD principles** when among others, building out its products, services and offerings which leverage on existing data sets held by the organization.

*****

Chun Hau Ng, Senior Associate, has contributed to this legal update.

Contact us

Serene Kan
Partner
serene.kan@wongpartners.com