ASL
CELEBRATING
50
YEARS

LEGAL UPDATE: MALAYSIA ISSUES THREE NEW PDPA GUIDELINES: ADMP, DPIA, AND DATA PROTECTION BY DESIGN

MONTH :
June 2026

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



LEGAL UPDATE: MALAYSIA ISSUES THREE NEW PDPA GUIDELINES: ADMP, DPIA, AND DATA PROTECTION BY DESIGN

On 30th April 2026, Malaysia's Personal Data Protection Commissioner (the "Commissioner") has issued three separate guidelines under the Personal Data Protection Act 2010 ("**PDPA**") on:-

(i) automated decision-making and profiling,
(ii) data protection impact assessments, and
(iii) data protection by design.

Although the subject matter will be familiar to many organizations, the guidelines consolidate the Commissioner's current practical expectations for managing higher-risk processing under the PDPA.

(1) Automated Decision-Making and Profiling ("ADMP"): explaining and governing algorithmic decisions

The Commissioner's guideline on Automated Decision-Making and Profiling addresses the increasing use of models, scoring systems, and other automated tools in decisions that may affect individuals. The guideline is focused on accountability—requiring organizations to be able to explain, manage, and justify automated or profiling-based processing, and to mitigate risks of unfair or adverse outcomes.

Threshold for application. Critically, the guideline applies where an automated decision produces legal effects on, or similarly significantly affects, a data subject, for example, decisions on credit, insurance, employment, education, pricing, or other outcomes that may cause material or reputational consequences. This threshold is what triggers the guideline's obligations, and organizations should assess each use case against it.

In practical terms, the guideline emphasizes three compliance disciplines. The first is transparency, including the ability to explain the role of automation and profiling and their effects on individuals. The second is governance and control, including clear internal rules on approvals, testing, monitoring, and escalation. The third is risk management, including treating automated decision-making and profiling as potentially higher-risk

processing that may warrant enhanced assessment and documentation, particularly where outcomes may materially affect individuals.

Preserved safeguards and the link to DPIAs. The guideline also preserves the existing data-subject safeguards under the PDPA, including the Notice and Choice Principle (section 7), the right to withdraw consent (section 38), the lawful bases for processing (such as the performance of a contract, compliance with a legal obligation, or the data subject's prior consent), and the additional protections for sensitive personal data (section 40). Importantly, automated decision-making and profiling are themselves treated as factors that trigger a Data Protection Impact Assessment regardless of the extent of processing, and the Data Protection Officer is expected to ensure that a DPIA is carried out for such processing.

AI best practices. Where artificial intelligence is used, the guideline sets out specific expectations: organizations should respect human dignity, train relevant staff, and guard against over-reliance on automated outputs; data subjects should be informed that AI is being used; and, critically, AI output must not be the sole factor in a decision that affects a data subject — meaningful human involvement is required.

Practical takeaway: Organizations should maintain a clear inventory of automated decision-making and profiling use cases, including the data inputs, decision logic (to the extent appropriate), and points of human oversight.

(2) Data Protection Impact Assessments ("DPIA"): formalizing risk-based compliance

The DPIA Guideline sets out a structured, risk-based approach: where a processing operation is likely to result in a high risk to the protection of personal data, the data controller is expected to conduct a DPIA to document the processing, identify risks, and record mitigation measures. The Guideline is expressly issued by the Commissioner pursuant to the Commissioner's functions under subsection 48(g) of the PDPA, and it is intended to be read together

with the PDPA and other relevant instruments issued under the PDPA.

When a DPIA is required: a two-tier test. The Guideline applies a two-tier assessment. A DPIA is required where the quantitative thresholds are met. Broadly, this is where the entity processes the personal data of more than 20,000 data subjects, or more than 10,000 data subjects when sensitive or financial data is involved. Where those thresholds are not met, controllers must still apply the qualitative factors, which include processing that has legal or similarly significant effects, systematic monitoring, the use of innovative technologies, the potential denial of rights, large-scale tracking of location or behaviour, the targeting of children or vulnerable individuals, and high-risk automated decision-making and profiling.

Operationally, the Guideline positions DPIAs as a governance mechanism to translate PDPA requirements into implementation decisions. It places the obligation to carry out a DPIA on the data controller (with support expected from processors where relevant) and emphasizes senior management accountability for DPIA outcomes. The Guideline also distinguishes between the Data Protection Officer ("DPO"), who supports and advises on DPIAs, and a designated "DPIA Lead" (who may be the DPO, a project manager, or other appropriate personnel) responsible for planning and execution.

A structured methodology. The Guideline prescribes a five-step methodology, sometimes referred to as "DEICA": describe the processing; evaluate its necessity and proportionality; identify the risks to data subjects; consider measures to mitigate those risks; and assess the residual risk, typically using a three-by-three risk matrix that scores likelihood against impact.

Validity, monitoring, and records. A DPIA is generally treated as valid for two years and should then be reviewed and refreshed, with continuous monitoring in the interim. Records should be retained for at least two years after the relevant processing ceases (often resulting in a retention period of around seven years overall) and should be made available to the Commissioner on request. Publication of a

redacted or summary version of a DPIA is encouraged as good practice but is not mandatory.

Practical takeaway: Organisations should expect DPIA documentation to become a key piece of documentation in regulatory engagement, especially for processing involving large-scale, sensitive data, innovative technologies, systematic monitoring, or automated decision-making and profiling that may have significant effects on individuals.

(3) 3) Data Protection by Design ("DPbD"): shifting privacy "left" into systems and workflows

The Commissioner's Data Protection by Design guideline frames DPbD as a proactive approach: embedding privacy and data protection controls into systems, products, and processes from the outset rather than attempting to retrofit compliance later.

What DPbD requires. In substance, Data Protection by Design means embedding technical and organizational measures that give effect to the Personal Data Protection Principles across the entire data lifecycle, from design and development through to deployment and decommissioning. The guideline is built around four elements: proactiveness; end-to-end protection; transparency; and user-centricity. It is structured by reference to the seven Personal Data Protection Principles (the General, Notice and Choice, Disclosure, Security, Retention, Data Integrity, and Access Principles) so that design measures can be mapped to each principle.

For many organizations, DPbD is less about a single control and more about embedding repeatable decisions into product and operational processes, such as, default retention settings, access controls, data minimization, purpose limitation, secure development practices, and auditability. The guideline reflects that approach by emphasizing early-stage consideration and internal processes that make privacy outcomes deliberate and consistent.

Patterns to avoid, and a risk-based posture. The guideline also identifies deceptive design patterns that organizations should avoid,

described as overloading, skipping, stirring, obstructing, fickle, and leaving the data subject in the dark. Finally, DPbD is expressed as non-mandatory and risk-based rather than prescriptive, so that the measures adopted should be tailored to the nature, size, and scope of the processing.

Practical takeaway: Even organizations that consider themselves "PDPA compliant" based on policies and notices may need to invest in engineering and product lifecycle controls to match DPbD expectations, particularly where personal data is core to product functionality.

How the three guidelines fit together: a governance through-line

Read together, the three guidelines reflect a single governance direction. The ADMP guideline addresses processing that is more difficult to justify without meaningful transparency and oversight. The DPIA guideline provides the discipline, an assessment and documentation process, to identify and manage risk before implementation. The DPbD guideline reinforces the expectation that privacy controls should be designed into products and workflows at the outset. The practical implication is that the Commissioner is focused not only on written compliance artifacts, but also on operational design and control.

What this means in practice

For organizations operating in Malaysia, the guidelines translate general PDPA concepts into operational expectations. As a baseline, organizations should map automated decision-making and profiling use cases (including vendor tools) and document where human oversight sits; implement a DPIA workflow that is triggered by higher-risk processing and embedded in business approvals; and embed data protection by design into the delivery lifecycle (requirements, design review, testing, release gates, and post-launch monitoring), rather than relying primarily on policies and notices.

Conclusion

The ADMP, DPIA, and DPbD guidelines are best understood not as three separate obligations but as one coherent direction of travel: the Commissioner expects accountability to be designed in, assessed in advance, and capable of being evidenced. Organizations that already maintain mature governance will find much of this familiar, but few will be

able to satisfy every expectation without revisiting their processes, documentation, and product lifecycle controls. The sensible response is to treat the guidelines as a prompt for a focused gap assessment now, prioritizing the higher-risk processing the Commissioner has signalled it cares about most, so that compliance is achieved deliberately rather than under pressure.

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, Michelle Yap Siew Hui and Emily Ong Wenyen (Managing Associate & Associates). 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.