

Deloitte.

**Adapting to Malaysia's DPO
Appointment Guidelines:
Outsource with Data Protection
Officer as a Service (DPOaaS)**

**MAKING AN
IMPACT THAT
MATTERS**
since 1845

Overview of DPO requirement

The Personal Data Protection (Amendment) Act 2024 introduced several major changes that demonstrate Malaysia's commitment to enhancing data privacy and protection. A key update is the mandatory appointment of a Data Protection Officer ("DPO").

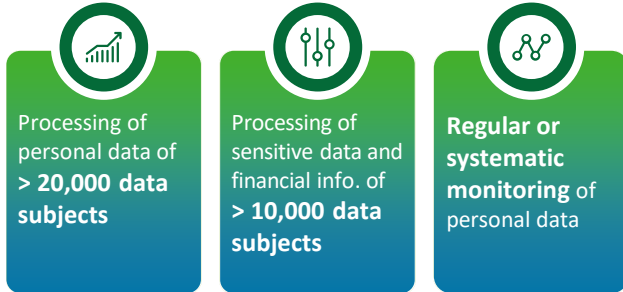
In line with this, the Malaysian Personal Data Protection Commissioner released a guideline¹ ("DPO Guideline") on 25 February 2025 to provide further clarity on the new obligation to appoint a DPO. The guideline¹ outlines the specific responsibilities of data controllers and processors, which takes effect from 1 June 2025.

Glossary:

- **Data Controller:** An entity that determines the purposes and means of processing personal data.
- **Data Processor:** An entity that processes personal data on behalf of the data controller, following its instructions.

Who needs to appoint a DPO?

A data controller or processor who satisfies the stated requirements are required to appoint one or more DPOs. The criteria are as follows:



Registration

A data controller is required to notify and register their DPO with the Commissioner:



Within 21 days

From the date of appointing the DPO

Changes to the DPO or the business contact information must be notified within **14 days**.

Business contact information

The data controller and, where applicable, data processor must **provide a dedicated business email** for the DPO and publish the DPO's contact information across all channels.

Roles and responsibilities (non-exhaustive)

The DPO should adopt a **risk-based approach** to privacy risk management and be **involved in all matters** related to personal data protection and the personal data lifecycle in a timely manner. The DPO can **serve multiple organisations**, provided they remain contactable through reasonable means and can respond within a reasonable timeframe. To note, the DPO **shall not be dismissed** except in cases of misconduct, negligence or breach of any applicable law.

Advise and aid organisations on their data processing and protection practices.

Support and monitor legal and regulatory compliance.

Develop data protection guidelines and conducting data protection impact assessments.

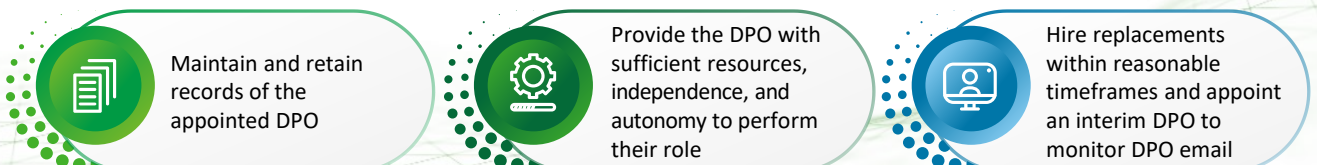
Promote and raise awareness for privacy in organisations. Conducting privacy training.

Report data breaches to Commissioner in accordance with prescribed timelines

Serve as the main liaison for Data Subjects and Commissioner.

Organisational responsibilities

The appointment of a DPO does not exempt both the data controller and processor from its compliance obligations. They remain responsible and liable for any regulatory non-compliance. Additionally, their responsibilities include the following:



Background and expertise

There are no minimum qualifications. However, DPOs should have sufficient training and skills through relevant courses and programs, and possess a strong understanding of the following areas:

Strong knowledge of MY PDPA and other applicable data protection requirements

Ability to **promote data protection culture** within the organisation



Understanding of organisation's data processing operations

Understanding of IT and data security

Ethical and professional integrity

The DPO requires greater expertise depending on the scale of sensitive data processing and the presence of systematic cross-border data transfers.

Language

The DPO must be proficient in **Bahasa Melayu** and **English**.







Residency

The DPO must be either a **resident in Malaysia** (i.e., physically present in Malaysia for at least 180 days in a calendar year) or **easily contactable** via reasonable means.

Differences between in-house DPO vs. outsourced DPO

According to Section 6.5 of the DPO Guidelines¹, there are two approaches to appointing a DPO. A DPO can be appointed from existing employees, or through outsourcing, e.g., DPO as a Service (“DPOaaS”) with a minimum term of at least two (2) years.

The table below highlights the key differences between an in-house DPO and an outsourced DPO, focusing on factors such as cost, expertise, scalability, and flexibility. This comparison serves as a guide to help organisations determine the most suitable governance model based on the organisation's specific requirements.

	In-house DPO	Outsourced DPO
Cost 	Higher upfront costs: <ul style="list-style-type: none"> Involves fixed costs such as salary, benefits, and training, which can be expensive, especially for smaller organisations. 	Lower costs: <ul style="list-style-type: none"> More cost-effective as the payment is subscription or contract-based. There is also no need to incur additional costs associated with employee benefits, training, or recruitment, as the service is provided externally.
Conflict of interest 	Potential risk: <ul style="list-style-type: none"> Higher likelihood of conflicts of interest, as the DPO may become too involved with internal functions or management, potentially influenced by internal politics and organisational pressures. 	Lower risk: <ul style="list-style-type: none"> More impartial, as they are external to the organisation and not influenced by internal dynamics or embedded within its structure.
Commitment 	Long-term: <ul style="list-style-type: none"> An in-house DPO is a long-term position, providing consistent leadership and deep knowledge of the organisation's operations, culture, and privacy risks. This continuity ensures effective management of data protection strategies, long-term accountability for compliance, and adaptability to evolving regulations and business needs. 	Short- to medium-term: <ul style="list-style-type: none"> More flexibility with short- to medium-term contracts that can be tailored to an organisation's needs, often with renewal options. Ideal for organisations with fluctuating data privacy and protection requirements or those in transitional phases, as it avoids the long-term commitment of an in-house DPO.
Scalability 	Limited: <ul style="list-style-type: none"> The capacity of an in-house DPO is limited by their workload and resources. As the organisation grows, the DPO may face increased demands, requiring additional staff or resources to support their role, leading to higher costs and administrative efforts. 	More scalable: <ul style="list-style-type: none"> Better scalability by allowing the outsourcing provider to allocate additional resources or adjust service levels in response to the organisation's changing needs. As the organisation expands or faces more complex data protection requirements, the service can be easily scaled up to accommodate increased workloads, additional jurisdictions, or evolving regulatory demands.
Expertise 	Specialised: <ul style="list-style-type: none"> In-house DPOs have a strong understanding of the organisation's operations, enabling them to tailor data privacy and protection strategies accordingly. However, they may require ongoing training to stay updated with evolving data protection laws, technological advancements, and global privacy standards. 	Generalised: <ul style="list-style-type: none"> External experts typically have broad industry experience, offering diverse perspectives in data protection. They are typically knowledgeable in multiple jurisdictions, helping organisations navigate and comply with regional and global privacy laws. This expertise ensures robust data privacy and protection practices and compliance with evolving international standards.
Availability 	Full-time: <ul style="list-style-type: none"> In-house DPOs are dedicated to managing and overseeing the organisation's data privacy and protection practices on an ongoing basis. As a permanent employee, they should be available to respond to the organisation's request during working hours or as required in times of emergency. 	Subject to contract terms: <ul style="list-style-type: none"> The availability of an outsourced DPO is governed by the terms in the service contract, which can vary in terms of access, response times, and service scope. Organisations can customise the service to meet their needs, whether for specific hours, business hours, or 24/7 support.

Positioning of the In-house DPO role

The DPO should be placed in a department that ensures effective oversight of data protection while considering the organisation's overall needs. The position of the DPO varies from one organisation to another, but is commonly placed within Legal, Compliance, IT, Risk Management, CISO, and Data Governance. Ultimately, the key is to ensure that the DPO has independence and direct access to senior management for effective execution of their responsibilities.

Legal department

Ensures that data protection practices are **aligned with legal requirements and regulations**, providing expert guidance on compliance matters

IT department

Ensures close collaboration on **technical aspects of data security**, enabling prompt identification and resolution of security vulnerabilities

CISO department

Allows the DPO to work closely with information security teams, ensuring that **data protection and cybersecurity** are **coordinated** for comprehensive risk management



Compliance department

Ensures that data protection policies and procedures are effectively **integrated** into the organisation's broader **compliance framework**

Risk management department

Proactively assess and **mitigate risks** associated with **data breaches** and ensure the organisation is **prepared** for potential data protection challenges

Data Governance department

Directly influence the organisation's **data management policies**, ensuring that data privacy is **embedded in data practices** from the outset

Governance models for in-house DPO

Generally, there are three governance models that organisations can structure their DPO function in, with each presenting its own set of advantages and challenges.

Centralised model

1



Holding company DPO function

Subsidiary A Subsidiary B Subsidiary C

Description

In a **centralised** model, a **single DPO** function **oversees all** the data privacy and protection matters across the organisation.

Pros

- Better **consistency** in terms of policies, procedures, and operationalisation across the organisation.
- **Streamlined** decision-making and **oversight**.

Cons

- **Limited flexibility** to address **local needs** as a central baseline will be adopted.
- May result in **slower responsiveness** to region-specific requirements.

Decentralised model

2



Holding company

Subsidiary A DPO function Subsidiary B DPO function Subsidiary C DPO function

A **decentralised** model assigns **multiple DPOs** or privacy teams **across** business units or regions.

- Provides **greater flexibility** and responsiveness to local requirements.
- **More autonomy** for individual business units or regions.

- Risk of **inconsistent policies** and practices across the organisation.
- Potential **inefficiencies** due to **fragmentation** of responsibilities.

Hybrid model

3



Holding company Head DPO function

Subsidiary A DPO function Subsidiary B DPO function Subsidiary C DPO function

A **hybrid** model combines elements of **both centralised** and **decentralised** approaches, with a **central DPO team** working closely with **local privacy officers** or teams across business units.

- Balances **consistency** with **local flexibility**.
- **Adaptable to varying regional needs** while maintaining core standards.

- Can be **complex to manage** and **coordinate** between central and local teams.
- Requires **clear communication** and **strong collaboration** to function effectively, to avoid any overlap.

About DPOaaS

This service involves outsourcing the role of a DPO to an external provider who manages compliance with data protection regulations, conducts risk assessments, oversees privacy policies, handles data subject requests, conducts privacy impact assessments, and provides staff training, ensuring robust data protection without the need for an in-house team. The table below outlines an illustrative and non-exhaustive list of activities involved in DPOaaS.

DPO responsibilities as per the Guidelines ¹	What Deloitte can do with DPOaaS
Section 8.2.1: Inform and provide advice on the processing of personal data	<ul style="list-style-type: none">• Provide advisory support on the management of personal data throughout the data lifecycle.• Develop or enhance the relevant framework, policies and procedures to govern the management of personal data throughout the data lifecycle.
Section 8.2.2 and Section 8.2.4: Support the data controller or data processor in complying with the PDPA and other related data protection laws, and monitoring the personal data compliance of the data controller or data processor	<ul style="list-style-type: none">• Conduct current state / gap / maturity assessment to evaluate the organisation's data privacy program, and framework, and propose recommendations to enhance overall maturity and compliance.• Operationalise the established privacy framework into day-to-day practices.• Develop self-monitoring mechanisms to ensure compliance with applicable laws, regulations and internal policy requirements.• Provide advisory support and develop training materials (incl. plans, communication strategies, and awareness content, etc.), and facilitate training sessions as required.
Section 8.2.3: Support the carrying out of Data Protection Impact Assessments	<ul style="list-style-type: none">• Workshop sessions with relevant stakeholders for the initial development of data inventories and data protection impact assessments ("DPIA").• Continuous maintenance of the data inventories and DPIA.
Section 8.2.5: Ensure proper data breach and security incident management	<ul style="list-style-type: none">• Development and conduct of data breach simulation exercise session• Standby and response time per month, with support for data breaches depending on their nature and scale.
Section 9.1: Act as a facilitator and point of contact between data subjects and the data controller or data processor regarding the processing of the data subject's personal data and their rights	<ul style="list-style-type: none">• Develop or enhance the organisation's data subject handling process.• Respond to data subject rights requests, and complaints / queries regarding data privacy and protection.• Standby and response time per month.
Section 10.1: Act as the liaison officer and the main point of reference between the data controller or data processor and the Commissioner	<ul style="list-style-type: none">• Provide helpdesk support by offering technical advice through call or email.• Standby and response time per month.

Our value proposition



Experienced in DPOaaS advisory

Our team has extensive experience in delivering DPOaaS, having successfully supported various organisations across diverse industries throughout Southeast Asia ("SEA"). This blend of industry-specific knowledge and practical experience positions us well to add valuable insights to the services we will provide.



Supplement your data privacy team

Most organisations have resource constraints and do not have a dedicated DPO. In such situations, balancing business-as-usual (BAU) operations and data privacy matters may get challenging. DPOaaS helps alleviate operational burdens and streamlines your data privacy team's activities.



Access to privacy experts to support you on demand

Most organisations struggle to operationalise their privacy policies as they may lack the required skills or expertise. Get access to our privacy experts who can advise you on operational matters and share the latest industry practices.



Have a DPO serving as a global or regional contact

Leveraging on Deloitte's global network of member firms, organisations can have one contact point for handling privacy matters.



No need for an in-house DPO

Small organisations may not be able to justify a DPO role from a cost perspective. You can outsource operational aspects of the DPO function to us.

Note: Organisations, seeking to outsource the DPO function to us through DPOaaS, are still required to formally appoint an internal stakeholder as a point of contact for the organisation.

Contact us



Ho Siew Kei
Cyber Risk Leader
Deloitte Malaysia
sieho@deloitte.com



Venkat Paruchuri
Data Privacy and Protection
Risk Leader
Deloitte Southeast Asia
veparuchuri@deloitte.com



Melvin Toh
Senior Manager, Technology &
Transformation
Deloitte Southeast Asia
mtoh@deloitte.com



Melbourne Lim
Manager, Technology &
Transformation
Deloitte Southeast Asia
melblim@deloitte.com

References

- 1 Personal Data Protection Guideline: Appointment of Data Protection Officer (DPO), Personal Data Protection Commissioner of Malaysia, 2025

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which is a separate and independent legal entity, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Bengaluru, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Mumbai, New Delhi, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

About Deloitte Malaysia

In Malaysia, services are provided by Deloitte Business Advisory Sdn Bhd and its affiliates.