



MANDATORY APPOINTMENT OF DATA PROTECTION OFFICER: WHAT ORGANISATIONS NEED TO KNOW

MONTH :

November 2025

BY :

Sri Sarguna Raj,
Steven Cheek Hou Cher
& Nicole Chong



MANDATORY APPOINTMENT OF DATA PROTECTION OFFICER: WHAT ORGANISATIONS NEED TO KNOW

Introduction

On 25 February 2025, the Personal Data Protection Department unveiled the Data Protection Officer Appointment Guidelines (“**DPO Guidelines**”) pursuant to the Personal Data Protection (Amendment) Act 2024. This marks a significant step forward in strengthening Malaysia’s data protection landscape. The DPO Guidelines set out the requirements and procedures for appointing Data Protection Officers (“**DPO**”). The DPO Guidelines officially take effect on 1 June 2025. Organisations and companies should take note of this mandatory obligation while ensuring that their internal policies and resources are

ready to meet the DPO appointment requirements. Below are some of the main highlights from the DPO Guidelines.

1. When Should I Appoint a DPO for My Company?

Pursuant to DPO Guidelines, the data controllers¹ and data processors² are required to appoint one or more data protection officers if their processing of personal data involves:

- personal data exceeding 20,000 data subjects;
- sensitive personal data³ (including financial information data) exceeding 10,000 data subjects; or
- involves activities that require regular and systematic monitoring of personal data.⁴

¹ Data controller is any person who processes any personal data or has control over or authorizes the processing of any personal data.

² Data controller is any person who processes the personal data solely on behalf of the data controller.

³ Sensitive personal data means any personal data consisting information of:

- i) physical or mental health or condition of a data subject;
- ii) political opinions;
- iii) religious beliefs or other beliefs of a similar nature;
- iv) the commission or alleged commission by him of any offence;
- v) biometric data; or
- vi) or any other personal data as the Minister may determine by order published in the Gazette.

⁴ Examples of regular and systematic monitoring of personal data: behavioral advertising, algorithms, CCTV, wearable devices and etc.

2. Who Should I Appoint as My Company's DPO?

Generally, there are no minimum professional qualifications for a person to be appointed as DPO. Yet, DPO Guidelines set out 5 key competencies for appointed DPO as follows:

- (i) **Knowledge of PDPA 2010** and any relevant data protection laws.
- (ii) **Familiarity of the data controller or data processor's business operations.**
- (iii) Competence of information technology and data security.
- (iv) **Personal qualities** such as integrity, understanding of corporate governance and high professional ethics.
- (v) Ability to foster **data protection culture** within the organisation.

Other Requirements for appointed DPO:

- DPO must be resident in Malaysia (i.e. be physically present in Malaysia for at least 180 days in one calendar year).

- DPO should be easily contactable.
- DPO should be proficient in Bahasa Melayu and English languages.
- Appointment should preferably be for a minimum of 2 years.
- Attend training programmes by the Personal Data Protection Commissioner (**"the Commissioner"**).

3. What are the Roles and Responsibilities of a DPO?

The roles of DPO include but not limited to the following:-

- Inform and advise the organisation on the processing of personal data.
- Support and monitor the data controller or data processor in complying with PDPA 2010 and data protection regulations.
- Support the organisation in carrying out Data Protection Impact Assessments determined by the Commissioner.

- Serve as the primary liaison officer and middle person between:

- (i) Data processor/data controller and data subjects; and
- (ii) Data processor/data controller and the Commissioner.

- Ensure that the organisation properly manages data breaches and security incidents by preparing reports and documents required by the Commissioner.

4. Should I Appoint a DPO from Within My Company or Outsource?

A DPO may be:

- Appointed from among existing employees of the company; or
- Outsourced via a service contract
 - (i) If outsourced with an organisation, the service agreement shall name the individual in the service contract as the lead contact and person in charge liaising with the

data controller or data processor.

- (ii) The service contract should clearly describe the duties and obligations of the DPO.

5. Do I Need to Notify the Commissioner About My DPO Appointment?

The data controller shall register the appointed data protection officer and submit their business contact information within 21 days from the date of appointment through the Personal Data Protection System (SPDP) via <https://daftar.pdp.gov.my>.

6. What Should I Do Next?

i) Determine Whether a DPO is Required

The first step for any organisation is to determine whether appointing a DPO is mandatory by referring to the DPO Guidelines. As such, if your organisation processes personal data for more than 20,000 individuals, or sensitive personal data for over 10,000 individuals, or involves activities that require

regular and systematic monitoring of personal data, you are required to appoint a DPO.

ii) Ascertain the DPO candidate

Once the need for a DPO is established, the next step is identifying a suitable candidate. Organisations may appoint an existing employee, commonly from the legal or human resources department, or choose to outsource the DPO function to an external professional or organisation with the requirements as explained above.

iii) Review Organisation Policies

After appointing a DPO, organisations should review and update their internal policies to clearly define the DPO's role, qualifications and responsibilities. These policies should also set out the DPO's reporting structure and detail the procedures for compliance monitoring, reporting, and communication within the organisation.

In addition, the organisation should update their official website, official media, personal data protection notices and security guidelines to include the DPO's business contact information, ensuring transparency and accessibility for data subjects.

By taking these steps, organisations can strengthen their data governance framework, foster a culture of accountability, and demonstrate their commitment to safeguarding personal data in compliance with Malaysia's evolving data protection landscape.

7. Conclusion

In summary, appointing a DPO is a crucial step in ensuring your organisation's compliance with data protection laws and maintaining trust with stakeholders. If you need guidance or support in fulfilling this requirement, our team is ready to assist. Contact us today to learn how we can help with your DPO appointment or outsourcing needs.

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, Lim Chaw Zen, Michelle Yap Siew Hui, Emily Ong Wenyen and Justin Ding Jiel Xin (Managing Associate, Associate & Pupils). 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.