MINISTRY OF DIGITAL

PERSONAL DATA PROTECTION GUIDELINE

APPOINTMENT OF DATA PROTECTION OFFICER

Version 1.0
Date of Issuance: 25 February 2025

Personal Data Protection Commissioner Malaysia

Address:

PERSONAL DATA PROTECTION COMMISSIONER OF MALAYSIA

Level 8, Galeria PjH, Jalan P4W, Persiaran Perdana

Precinct 4, Federal Government Administration Centre

62100 Putrajaya, Malaysia

TABLE OF CONTENTS

PART A: INTRODUCTION

1 Background

1.1 Section 12A of the Personal Data Protection Act 2010 ("**Act 709**") sets the requirement for both data controller and data processor to appoint one or more data protection officer to oversee their compliance with Act 709.

1.2 This Guideline sets out the requirements to appoint data protection officer, roles and responsibilities of the data protection officer and obligations of the data controller and data processor to ensure the effective implementation of the data protection officer's role in compliance and in accordance with the Act 709.

1.3 Please note that examples provided in this Guideline are not intended to be exhaustive and are only included for context and for purposes of illustration.

1.4 This Guideline is to be read together with Act 709, Circular of Personal Data Protection Commissioner No. 1/2025 (Appointment of Data Protection Officer) ("**Circular No. 1/2025**"), and any other relevant legislative instruments issued under the Act 709. This Guideline does not override any other specific data protection laws or data protection regulations in effect at any given time.

2 Legal Provisions

2.1 This Guideline is issued by the Personal Data Protection Commissioner ("**Commissioner**") pursuant to the function and responsibilities of the Commissioner under subsection 48(g) of the Act 709.

3 Interpretations

3.1 Unless otherwise defined in this Guideline, the terms and expressions used herein shall have the same meanings as those assigned to them under the Act 709, the Circular No. 1/2025, and any other relevant legislative instruments under the Act 709.

3.2 In this Guideline, unless the context otherwise requires:

"**business contact information**"	means an individual's name, position or title, business telephone number, business address, the dedicated and official business e-mail address or business fax number and any other similar information about the individual, not provided by the individual solely for his or her personal purposes.

PART B: REQUIREMENTS FOR THE APPOINTMENT OF DATA PROTECTION OFFICER

4 Conditions for the Appointment of Data Protection Officer

4.1 Under the Circular No. 1/2025, the requirement for the appointment of data protection officer is subject to the conditions determined by the Commissioner.

4.2 In accordance to the section 12A of Act 709, data controller and data processor are required to appoint one or more data protection officers if their processing of personal data involves:

4.2.1 personal data exceeding 20,000 data subjects;

4.2.2 sensitive personal data including financial information data exceeding 10,000 data subjects; or

4.2.3 involves activities that require regular and systematic monitoring of personal data.

4.3 For the purposes of determining "*regular and systematic monitoring*" in paragraph 4.2.3 above, below are some examples for reference:

Examples:

- Any form of activity where data subjects are tracked and profiled online or offline for purposes of behavioural advertising will be considered as activities which require regular and systematic monitoring.

- A retail website that uses algorithms to monitor the searches and purchases of its users and based on this information, offers recommendations to them, would be carrying out "*regular and systematic monitoring*" of data subjects.

- Data controller or data processor that carry out activities such as:

  - operating a telecommunications network;

  - monitoring the wellness, fitness and health data via wearable devices; and / or

  - activities involving Close-Circuit Television (CCTV) or connected devices such as smart cars, home automation system etc.,

  would be considered as carrying out activities that may constitute "*regular and systematic monitoring*".

- The management of loyalty programme may not be considered as activities that require "*regular and systematic monitoring*" of the data subjects if the purpose of doing so was strictly to manage the data subjects' accounts and not to monitor their purchase behaviours.

4.4 Notwithstanding Para 4.2, data controller or data processor shall notify the Commissioner on the appointment of data protection officer if there is any urgency.

4.5 Data controller or data processor may keep a record on the reasons for not appointing data protection officer if they find the requirements in para 4.2 are not fulfilled.

5 Expertise and Qualifications of Data Protection Officer

5.1 Data controller or data processor must ensure that the appointed data protection officer is able to adequately carry out their tasks.

5.2 Subject to paragraphs 5.6 and 5.7 below, data controller and data processor shall determine appropriate level of qualifications, experiences, skills and expertise required for data protection officer taking into consideration:

5.2.1 the operation of personal data processing being carried out;

5.2.2 the complexity and scale of data processed;

5.2.3 the sensitivity of the personal data processed; and

5.2.4 the level of protection required for the data being processed.

5.3 The appointed data protection officer needs to possess a higher level of skill and expertise and support from the data controller or data processor depending on factors such as:

5.3.1 the scale of sensitive personal data being processed; or

5.3.2 involved in complex processing of personal data such as systematic personal data sharing between multiple organisations and cross-border personal data transfers.

Minimum Skills or Expertise

5.4 There are no minimum professional qualifications required prior to being appointed as a data protection officer, unless the data controller or data processor or the Commissioner otherwise determines from time to time.

5.5 In any event, the data controller or data processor must ensure that the appointed data protection officer can demonstrate a sound level of the following skills, qualities and expertise:

5.5.1 knowledge on the Act 709, requirement under the law data protection practices in the country (including any other applicable data protection laws, where relevant);

5.5.2 understanding of the data controller or data processor's business operations and the personal data processing operations that are carried out;

5.5.3 understanding of information technology and data security;

5.5.4 personal qualities such as integrity, understanding of corporate governance and high professional ethics;

5.5.5 ability to promote data protection culture within the organisation;

Data Protection Officer Training

5.6 In order to ensure that appointed data protection officer has the knowledge, skills and expertise required to perform his duties efficiently, the Commissioner may decide necessary or expedient mechanisms such as determining courses and training programmes including professional skills benchmarking mechanisms and other relevant programme for data protection officer.

5.7 Data controller or data processor must ensure that appointed data protection officer has sufficient training and skills to carry out duties as data protection officer efficiently by attending the relevant courses or training programmes.

6 Matters Relating to the Appointment of Data Protection Officer

6.1 The appointment of data protection officer shall not discharge data controller or data processor from the obligations to ensure compliance with the requirements of the Act 709 when processing personal data. The data controller or data processor remains responsible and liable for any non-compliance with the provisions under the Act 709.

6.2 A data protection officer may execute other official duties and responsibilities or perform additional tasks as part of his job scope, such as a legal counsel, risk management officer etc. However, the data controller or data processor shall ensure that the performance of such other tasks and functions does not cause a conflict of interest to the data protection officer.

Examples:

- A data controller or data processor's Head of Marketing is asked to carry out a marketing campaign to promote the data controller or data processor's products and accept a dual role as a data protection officer within the company. The head of marketing should not accept the role of data protection officer as the objective is to:

  (i) target as many customers as possible and process their personal data for direct marketing purposes; and

  (ii) maximise product sales, may conflict with the data protection officer's role in the organisation in ensuring compliance with the Act 709 and safeguarding customer's personal data.

- Roles such as records manager or compliance officer, are generally less likely to result in conflict of interest as these roles focus on ensuring compliance with personal data protection rights.

6.3 The data protection officer's position may be a part-time or full-time role, taking into account the organisation's function, structure and size.

6.4 In the event that an individual appointed as the data protection officer ceases their service or reaches the end of their term, the data controller or data processor shall appoint, reappoint, or hire a replacement within a reasonable time frame. The data controller and data processor shall, as soon as possible, appoint an interim data protection officer to monitor communications in the official business e-mail of the data protection officer.

Method of Appointing Data Protection Officer

6.5 Data protection officer may be appointed from among existing employees or through outsourcing services (based on a service contract signed with an individual or organisation).

6.6 Where the data protection officer is appointed through a contract, data controller or data processor is recommended to ensure that the appointment is for a term of at least two (2) years, to ensure stability.

6.7 Data controller or data processor that appoints external data protection officer must clearly, concisely and comprehensively describe the duties and obligations of the data protection officer in the service contract.

6.8 Data controller or data processor must ensure that the appointed outsource organisation designate an individual within the organisation as the lead contact and person-in-charge ("**PIC**") for liaising with the data controller or data

processor. This lead contact or PIC must be specified / referenced in the service contract with the external service provider.

Accessibility of Data Protection Officer

6.9 A data protection officer may be appointed to serve multiple data controllers or data processors, provided that the data protection officer is easily accessible by the different entities receiving the data protection officer's service.

6.10 For better responsiveness and accessibility, it is required that the data protection officer:

6.10.1 be resident in Malaysia (i.e. be physically present in Malaysia for at least 180 days in one calendar year); or

6.10.2 easily contactable via any means; and

6.10.3 be proficient in the Bahasa Melayu and English languages.

7 Notification of Data Protection Officer Appointment

7.1 Data controller that fulfills the conditions for appointing data protection officer shall register the appointed data protection officer and submit their business contact information within twenty-one (21) days from the date of appointment.

7.2 Notification to the Commissioner regarding the appointment of the data protection officer shall be submitted through the Personal Data Protection System (SPDP) via https://daftar.pdp.gov.my.

7.3 The business contact information shall be duly maintained and promptly updated by the data controller to ensure efficient communication with the data protection officer can be made at all reasonable times.

7.4 If there is a change in the appointed data protection officer or the business contact information of the data protection officer, the data controller shall promptly maintain and update the changes no later than fourteen (14) days from the effective date of the new appointment via SPDP.

PART C: THE ROLES OF DATA PROTECTION OFFICER

8 Responsibilities of Data Protection Officer in relation to the Appointing Data Controller or Data Processor

8.1 In performing his duties, data protection officer shall adopt a risk-based approach in assessing risks from the perspective of the data controller or data processor's processing operations, taking into account the nature, scope, context and purposes of the processing. He shall also coordinate and cooperate with relevant personnel of the data controller or data processor as necessary.

8.2 Data protection officer shall have at least the following core responsibilities in respect of the data processing activities of the data controller or data processor:

8.2.1 inform and provide advice to the data controller or data processor on the processing of personal data;

Examples:

- educating the data controller or data processor regarding the requirements under Act 709 applicable to its personal data processing activities.

- advising the data controller or data processor regarding different laws, regulations and related instruments, as well as industry standards and certifications for ensuring adequate compliance with personal data protection requirements.

8.2.2 support the data controller or data processor in complying with Act 709 and other related data protection laws including staying informed of data processing risks affecting the data controller or data processor;

Examples:

- collect information to identify the processing operations, activities, measures, policies or systems of the data controller or data processor and maintain a record thereof.

- advise and oversee the implementation of security measures to protect personal data from unauthorised access, disclosure, alteration or destruction, in line with both legal requirements and internal security policies.

- advise the data controller or data processor on the potential risks and impacts that may arise from the data controller or data processor's business practices.

- develop, review and/or revise the data controller or data processor's data protection policies, guidelines etc.

- consider the adoption of accreditations or certifications to demonstrate the personal data processing standards implemented by the data controller or data processor.

- advise the data controller or data processor on the necessity of executing binding agreements with third parties (e.g. data transfer agreements, sub-processing agreement etc.).

8.2.3 support the carrying out of Data Protection Impact Assessments in accordance with the requirements as may be determined by the Commissioner from time to time;

8.2.4 monitor the personal data compliance of the data controller or data processor;

Examples:

- analysing and investigating compliance of the data controller or data processor's processing activities.
- assigning and delegating responsibilities under the data controller or data processor's data protection policies to promote accountability and comprehensive supervision.
- raising awareness and training employees on the data protection requirements of the data controller or data processor.
- conducting audits on the compliance of the data controller or data processor with their data protection policies and requirements.
- issuing recommendations to close any compliance gaps that have been identified.

8.2.5 ensure proper data breach and security incident management by assisting the data controller or data processor to prepare, process and submit reports and other documents required by the Commissioner in respect of personal data breaches, within the prescribed periods; and

8.2.6 such additional responsibilities that the Commissioner or the data controller or data processor may include from time to time (e.g. as a result of technological developments).

9 Responsibilities of Data Protection Officer in relation to Data Subjects

9.1 The data protection officer shall 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.

Examples:

- handle issues related to the processing of data subject's personal data (e.g. complaints).
- manage requests concerning the exercise of the data subject's rights (e.g. requests to correct and access personal data).
- educate data subjects about the processing of their personal data (e.g. informing data subjects about the purposes for processing their personal data, the third parties to whom their personal data is disclosed and their rights).
- Act as the contact point for data subjects in cases of personal data breaches and address any concerns that may arise from data subjects.

10 Responsibilities of Data Protection Officer in relation to the Commissioner

10.1 The Data Protection Officer shall act as the liaison officer and the main point of reference between the data controller or data processor and the Commissioner.

Examples:

- serves as the primary liaison officer between the data controller or data processor and the Commissioner.

- facilitate access to documents and information during inspections or investigations into the personal data processing activities of the data controller or data processor conducted by the Commissioner.

- prepare and submit information required by the Commissioner on any personal data breaches, in accordance with prescribed timelines.

- represent the data controller or data processor in industry engagement sessions or programme organised by the Commissioner.

11 Independence of Data Protection Officer

11.1 Data controller or data processor must ensure that the data protection officer is provided with the necessary resources, as outlined in paragraph 14 of these Guidelines, to enable them to perform their functions with sufficient independence and autonomy.

11.2 To safeguard the independence of the data protection officer, the data controller or data processor shall strive to avoid placing the data protection officer in a positions that could cause conflict between business interests and compliance with Act 709.

11.3 Data protection officer should have direct reporting access to senior management (or its equivalent) of the data controller or data processor.

12 Term of Service of Data Protection Officer

12.1 Data protection officer is accountable to the data controller or data processor who have appointed the data protection officer for compliance with Act 709.

12.2 Data protection officer shall not be dismissed by the data controller or data processor for performing his duties in good faith, unless the data protection officer has breached applicable laws and/or been found to have committed negligence or misconduct.

PART D: RESPONSIBILITIES OF DATA CONTROLLER AND DATA PROCESSOR

13 Involvement of Data Protection Officer

13.1 The data controller or data processor shall ensure that the data protection officer is involved in all matters related to the protection of personal data in a timely manner.

13.2 To ensure the timely involvement of the data protection officer, the data controller or data processor must engage the data protection officer in all matters related to data protection, starting from the earliest stage of the data processing lifecycle, that is from policy formulation to the collection, storage and deletion or destruction of personal data.

Examples:

- Data protection officer should be included in senior management / board meetings or relevant working groups to discuss the governance of personal data protection across the entire organisation of the data controller or data processor.

- Data protection officer must be provided with the necessary and sufficient information promptly to effectively carry out their functions.

- The views of the data protection officer should be sought as soon as the organisation's activities are reasonably considered to have implications for or

be impacted by the data processing activities of the data controller or data processor organisation.

- Data protection officer must be promptly informed and consulted in the event of a data breach or similar security incidents.

13.3 As a recommended practice, the data controller or data processor may develop data protection guidelines as an addition to the security policy, outlining scenarios in which the data protection officer's involvement is required, and disseminate these guidelines throughout the organisation.

14 Allocation of Resources to Data Protection Officer

14.1 Data controller or data processor must ensure that data protection officer is provided with adequate resources to carry out tasks effectively.

14.2 When assessing the adequacy of the resources to be provided, the data controller or data processor should consider factors such as the complexity of the data processing operations, the sensitivity of the personal data being processed and the size and structure of the organisation.

14.3 The resources that data controller or data processor may provide to support the data protection officer’s functions should be considered comprehensively.

Examples:

The following are examples of resources / support that data protection officer may receive from data controller or data processor:

- The data protection officer receives support from top management and the board of directors in carrying out his functions and responsibilities.

- The data protection officer is allocated sufficient time to perform his duties, taking into account whether his appointment is on a part-time or full-time basis, as well as whether he undertakes other tasks aside from those designated for his role.

- The data protection officer is granted access to other services such as human resources, legal, information technology, security and others to ensure they receive the necessary support, input and information from these services.

- The data protection officer is provided with adequate support in the form of financial resources, infrastructure (premises, facilities, equipment), and manpower. Depending on the size and structure of the organisation, there may be a need to establish a support team led by the data protection officer to ensure that their functions and responsibilities are carried out effectively.

- The data controller or data processor formally acknowledges the role of the data protection officer by issuing a notice to all employees within the organisation to ensure awareness and understanding of the data protection officer's existence and functions.

- The data controller or data processor provides the data protection officer with continuous recognised training in order to ensure professional development.

15 Publication and Communication of the Contact Details of Data Protection Officer

15.1 Data controller and data processor shall create a dedicated official business e-mail account for the data protection officer. This official business e-mail account must be actively monitored and maintained at all times to ensure clear, effective and seamless communication between data protection officer, Commissioner and data subjects. The dedicated official e-mail account created shall be distinct and

separate from the personal and official business work e-mail address of the individual appointed as a data protection officer.

15.2 Data controller or data processor shall publish the business contact information of the data protection officer through any or all of the following methods / channels:

15.2.1 the official website and other official media of the data controller or data processor;

15.2.2 personal data protection notices;

15.2.3 security policies and guidelines.

15.3 The official media of the data controller or data processor includes channels such as social media platforms, intranet, telephone directories, and other relevant mediums.

16 Record Keeping

16.1 Data controller or data processor shall accurately maintain and retain records of the appointed data protection officer to demonstrate compliance with the Act 709.