AITI
Authority for Info-communications Technology Industry of Brunei Darussalam

GUIDE

Appointment of Data Protection Officers

Version 1.0 | 4 June 2025

Contents

1. Introduction

1.1 Section 7 of the Personal Data Protection Order, 2025 **("PDPO")** sets out the requirement on the responsibilities of organisations through accountability-driven policies, practices and processes of data protection by private sector organisations in Brunei Darussalam.

1.2 The PDPO requires an organisation to designate one or more individuals to be responsible for ensuring that the organisation complies with the law. This individual is typically referred to as the **Data Protection Officer ("DPO").**

1.3 The Guide has been developed by the Authority for Info-communications Technology Industry of Brunei Darussalam **("AITI")** to provide a baseline set of considerations on the appointment of DPOs, including their expertise, skills, roles and responsibilities to ensure the effective implementation of data protection policies and practices. Such considerations play an important role in the efforts to build a safe and trusted digital ecosystem in Brunei Darussalam.

1.4 Note: The illustrations provided in this Guide are not intended to be exhaustive and are only included as examples for the specified paragraph.

2. Appointment of the Data Protection Officer

2.1. The Data Protection Officer plays an essential role in facilitating compliance to the PDPO and it is imperative for organisations to appoint a suitable candidate. The following sections cover clarifications on the level of expertise and skills of the DPO as well as the types of business contact Information to be made available to the public.

Expertise and Skills of the DPO

2.2. Organisations must ensure that it appoints at least one (1) individual to be designated as the DPO. This individual should be sufficiently skilled and knowledgeable in data protection and amply empowered to discharge their duties as a DPO.

2.3. The sufficient level of skills and knowledge of the DPO should be determined in accordance to the data processing operations carried out by the organisation, the complexity and amount of personal data, the cross-border transfers of data and the protection required for the personal data being processed

2.4. The PDPO does not prescribe any specific professional qualifications for the DPO but the individual is expected to have the following qualities:

(a) a good understanding of the personal data processing operations carried out;

(b) a sound knowledge of the relevant data protection laws and practices, including the PDPO;

(c) an understanding of information technology, data security and corporate governance practices;

(d) ability to cultivate a culture of accountability within the organisation, in particular amongst staff which directly handles personal data of individuals; and

(e) conducts work with integrity and high professional ethics.

2.5. Organisations must ensure that their DPO attends relevant courses or training programmes in order to be perform their duties effectively.

2.6. The individual designated as the DPO should ideally be a member of the organisation's senior management team or have a direct reporting line to the senior management to ensure the effective development and implementation of the organisation's data protection policies and practices. The commitment and involvement of senior management is key to ensure that there is accountability and oversight over the management of personal data in the organisation.

2.7. Organisations may appoint an existing employee or a new hire or alternatively, outsource the function to an external entity altogether.

(a) For existing employees, organisations shall ensure that there is no conflict of interest when performing their other official duties and responsibilities within their job scope.
(b) For outsourced DPO(s), it is recommended to specify within the service contract matters relating to the designation of a single individual as the organisation's assigned lead DPO, the duration of such designation and the allocation of tasks.

Illustration on the appointment of an existing employee as a Data Protection Officer
(Reference is made to Para 2.7(a))

Organisation A is an e-commerce company which collects, uses, discloses and processes personal data of its customers in order to provide online shopping services. Based on the organisation's assessment of its data processing activities and the organisational structure, both the Marketing Officer and Legal Officer have played a role in determining the purposes and means of processing of personal data of their customers.

The organisation appointed the Compliance Officer as the DPO as he is independent from such activities and has a good understanding of corporate governance and data protection practices. The organisation also ensures he is able to give sufficient time to perform dual roles effectively in his duties within his department and as the appointed DPO.

Illustration on the appointment of a Regional Data Protection Officer
(Reference is made to Para 2.7(a))

Organisation B is a financial institution with presence in Brunei Darussalam and Malaysia. Based on the organisation's assessment of its data processing activities and its current strategic priorities, it has decided that it will designate the same Data Protection Officer, based in their headquarters in Malaysia, to also oversee data protection matters for their Brunei Darussalam branch.

The organisation appointed this individual as their Regional Data Protection Officer for both branches. It also ensures that the DPO's business contact information is made available on the website and is able to respond within Brunei Darussalam's business hours.

Illustration on the appointment of an outsourced Data Protection Officer
(Reference is made to Para 2.7(b))

Organisation C is a private clinic which collects, use, discloses and processes personal data of its patients in order to provide healthcare services. Based on the organisation's assessment of its data processing activities and its small-scale operations, it has decided to engage an external DPO-as-a-service provider with data protection experience in the healthcare industry.

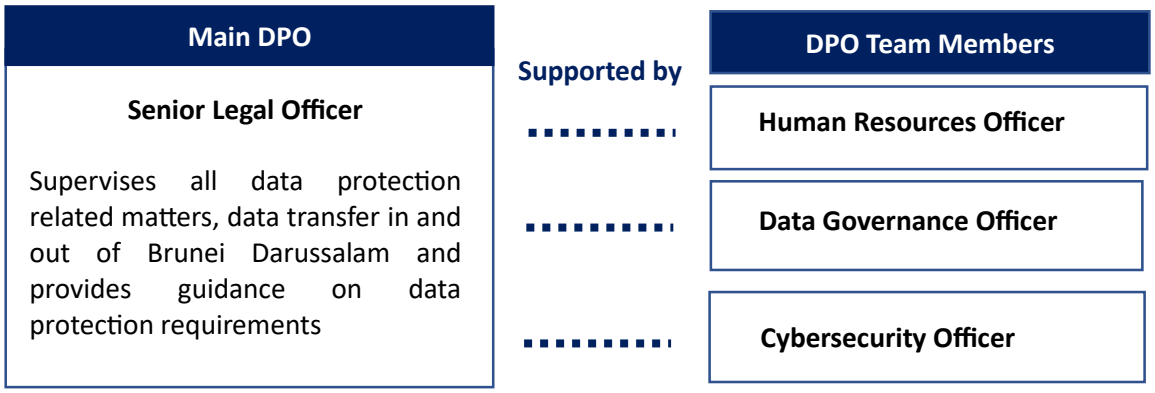
The organisation appointed an outsourced DPO, where it has taken steps to ensure that there is a service contract which clearly assigns (i) the designated individual as the lead DPO and the main focal point for organisation C, (ii) the duration of their designation and (iii) the clear allocation of tasks in order to perform duties as their DPO effectively.

2.8 It is worth noting that the appointment of an individual as the organisation's DPO does not relieve the organisation of any of its obligations under the PDPO. Thereby, the responsibility for complying with the PDPO still remains with the organisation and is not transferred to the designated individual(s).

2.9 Larger organisations may find it suitable to appoint more than one individual to form a DPO team comprising of one main DPO with supporting roles from other relevant functions. This acts as a cross-functional team where they would be able to collectively ensure the alignment and compliance with the PDPO, as well as project requirements and applicable industry standards.

Illustration on the appointment of DPO team within an organisation
(Reference is made to Para 2.9)

Organisation D is an investment group which collects and processes personal data of the employees of all its five subsidiary companies in a centralised system. Based on Organisation D's assessment of its data processing activities and the scale of the personal data held, the organisation has decided to form a DPO team through the following structure:



The organisation appointed the Senior Legal Officer as the main DPO, with support from the Human Resources Officer, Data Governance Officer and Cybersecurity Officer. Collectively, the DPO team co-operated to ensure proper data protection processes are in place including reasonable security measures and restricted access controls of assigned staff in each organisation. The DPO team also conducts regular meetings in order to keep up to date with any related developments to the data flows relating to system.

Business Contact Information

2.10 Organisations are required to make the Business Contact Information **("BCI")** of an individual available to the public in accordance to his duties as the DPO[1] and to respond to request for the access or correction of personal data.[2] In this respect, organisations may choose to make available the BCI of the same individual or any other individual designated as part of the DPO team. Hence the DPO, or someone within the DPO team, can be the primary contact point for the organisation's data protection matters.

2.11 Business Contact Information includes job designation, business telephone number, business address and a designated e-mail address of the DPO.

2.12 Organisations may publish the BCI through any of the following methods:

(a) on the official website or other official media channels;
(b) any data protection notices or policy statements;
(c) on-premise notices; and/or
(d) a dedicated contact form addressed to the DPO.

2.13 To ensure the ease of contact, the BCI should be provided in a readily accessible part of the organisation's official channels or notices. For those operating in physical stores only, it is equally important to display the BCI clearly within the premises, such as on a customer service counter. This ensures that customers visiting the store can easily find assistance or make inquiries.

2.14 The BCI provided should be operational during Brunei Darussalam's business hours with registered Brunei Darussalam telephone numbers.

2.15 While the name of the DPO is not required to be published, it is recommended to be communicated within the organisation, as well as to AITI.[3] Any changes to the appointed DPO or his BCI should be updated and informed to AITI no later than seven (7) working days from the effective date of the new appointment.

Illustration on Business Contact Information
(Reference is made to Para 2.12(a))

Organisation E is an insurance company which has appointed an individual from the legal department as their DPO based on their sound knowledge of data protection laws. It has published on the website the DPO's name, their designation as the DPO and a dedicated email to respond to data protection enquiries called dpo@insurancecompany.com.

[1] Section 7(1)(d) of the PDPO.
[2] Section 17(1)(c) and 17(6)(b) of the PDPO.
[3] For the purpose of acting as a focal point between the organisation and AITI on data protection matters.

3. Roles and Responsibilities of the Data Protection Officer

3.1. When assessing the suitability of a DPO candidate, the organisation must also understand the key roles and responsibilities entrusted to the DPO as it will form as part of the organisation's accountability in the personal data under their possession or control. The following section cover the key responsibilities of the DPO.

3.2. An organisation's DPO plays an essential role in how the organisation meets its obligations under the PDPO and generally acts as the primary internal expert on data protection.

3.3. The DPO can facilitate the organisation's compliance to the PDPO through the following core responsibilities:[4]

(a) To develop and implement data protection policies and practices;
(b) To develop complaints handling process on data protection matters;
(c) To communicate the organisation's data protection policies and practices to its staff; and
(d) To publish data protection policies and practices and complaints handling process, upon request.

3.4. An organisation's personal data protection policies and practices set the tone for the organisation's management of personal data, and provide clarity on the direction and manner in which an organisation manages personal data protection risks, based on its specific business or organisational needs.

3.5. The DPO should take steps to ensure that the organisation informs all relevant stakeholders of the purposes for collection, use and disclosure of personal data. In general, this can consist of developing an internal data protection policy for employees and an external data protection policy for customers.

3.6. In performing their duties, the DPO should consider a holistic approach by coordinating with relevant internal staff as well as any third-party organisations, such as vendors, contractors or service providers, which are involved in the processing of personal data on behalf of the organisation.

[4] Section 7(1)(e) of the PDPO.

3.7. The DPO should also act as the focal point to facilitate communication of data protection matters to the following stakeholders:

(a) **Focal point to individuals**
The DPO should acknowledge and respond in a timely manner to any enquiries, complaints or request of access or correction by an individual in relation to their personal data.

(b) **Focal point to AITI**
The DPO should represent the organisation in AITI's industry stakeholder consultations, training and awareness programmes as well as facilitate the reporting of data breach incidents and submission of relevant documents

3.8. The responsibilities of the DPO often include working with senior management as they are expected to be able to provide sound advice on the recommended data protection measures.

3.9. The DPO should be actively engaged when there are possible implications on data protection and it is thereby essential to involve and consult the DPO early in the relevant business processes and systems. Their early involvement is important from the outset when conducting data inventory and impact assessments as well as establishing appropriate processes to mitigate any data breach incidents.

3.10. Amongst other duties, the DPO should assist in cultivating a culture of accountability within the organisation and regularly communicate the organisation's data protection policies and processes to all stakeholders.

Illustration on Responsibilities of DPO in relation to data protection policies and practices.
(Reference is made to Para 3.3(a) and (d))

Organisation F is a new payment service provider which collects and processes personal data of customers in order to facilitate financial transactions between its clients and customers. Based on the organisation's assessment of the potential type and amount of personal data to be processed, it recognises the need to develop and implement an external Data Protection Policy.

The DPO gathered the relevant stakeholders involved in the development of the system, its operations and management of personal data. The DPO addressed the purpose of the policy, its intended audience and sought for clarification on the purposes for the collection and processing of personal data.

The DPO ensures that the necessary data protection processes have been established and published the organisation's Data Protection Policy on its official website.

Illustration on Responsibilities of the DPO in relation to complaints handling processes.
(Reference is made to Para 3.3(b) and (d))

Organisation G is a real estate company which collects and processes personal data through an online contact form for the viewing of a residential property only. The organisation included the DPO's business contact information on the website for any data protection enquiries and complaints which may arise, such as using the provided information for marketing which is beyond the original purpose.

Upon receiving a complaint, the DPO responds as soon as reasonably possible to acknowledge receipt and informs the individual of the actions that will be taken to handle the complaint. The DPO further engages the relevant unit to address the necessary data protection measures that needs to be established within a reasonable period. Thereafter, the DPO informs the individual that the complaint has been processed and appropriate actions have been taken.

Illustration on the Responsibilities of the DPO in relation to communication of data protection policies and practices to its staff.
(Reference is made to Para 3.3(c))

Organisation H is a charitable organisation which collects and discloses personal data of individuals which will receive support in the form of donated goods.

The DPO ensures that it has dedicated time to train and educate all staff on the organisation's data protection policies and practices. As the organisation also handles personal data of vulnerable individuals, the DPO has taken steps to also ensure it also communicates the importance of safeguarding such information and its policies to any its volunteers and other entities involved.

4. Accountability Tools

4.1. Although it is not expressly required under the PDPO, there are general data protection tools which organisations may find useful to in order to demonstrate good data management practices and accountability in the personal data under their possession or control. The following tools provides best practices in which organisations may want to follow:

4.1.1. Adoption of a Data Protection by Design approach

(a) Data Protection by Design ("DPbD") is a proactive and preventive approach to manage risks by considering potential data protection issues of any system, product, services and processes and addressing these risks throughout the data lifecycle.

(b) Organisations can take steps to ensure the safeguarding of individuals' personal data by embedding data protection principles as an integral part in the design and architecture stage.

(c) The data protection functionalities should be set as default and aim to benefit the users with respect to rights of individuals under any applicable data protection laws.

(d) Strong security measures should be considered throughout the entire data lifecycle, from the collection and storage of the data to processing and disposal of the data.

(e) This approach may help organisations to avoid any delays or additional costs that may be incurred if data protection risks are addressed at a later stage.

(f) For existing systems, organisations may want to thoroughly review the processes by considering the types and amount of personal data involved and enhance such system to address the potential risks with data protection measures.

(g) Generally, the DPbD approach can be implemented by IT project managers, system architects and software developers involved in the development of such systems, with the assistance of the DPO.

Illustration on adopting Data Protection by Design principles to a new system
(Reference is made to 4.1.1(a))

Organisation I is a logistics company which collects and stores personal data of its employees. As it is expanding, it intends to transition the storage of employee data from physical files to a new human resource management system which can streamline the administration process of its employees.

The IT project manager involves the DPO in the early design stage of the new system in order to ensure data protection principles are considered, such as ensuring its functionalities allow for the restriction of access controls to assigned staff only at an assigned period. The DPO also assists in making sure only necessary fields of information are requested and to make it clear to employees which fields are required or optional.

4.1.2. **Producing a Data Inventory Map**

(a) A Data Inventory Map is a type of data mapping which identifies the data assets and the flows of data relating to a system or process.

(b) It maps out the types of personal data, the purposes of its collection, the access controls, the methods of transfer, the types of storage and the disposal method.

(c) It captures the processes by mapping the flow of data including the assigned staff involved in the management of personal data ranging from internal departments or external third-party organisations.

(d) Organisations should review and update its inventory map periodically along with any developments relating to the system or processes.

(e) Generally, the data inventory map can be implemented by project managers involved in the development of the system or process, with the assistance of the DPO.

4.1.3. **Conducting Data Protection Impact Assessment**

(a) Data Protection Impact Assessment ("**DPIA**") is a type of assessment which organisations can conduct prior to or during the planning stages of any new project to identify, evaluate and address personal data protection risks from their business and operational processes.

(i) **Stage 1: Assess the need for a DPIA**
Organisations may first determine whether there is a need to conduct a DPIA for a system based on the scale of the collection, use, disclosure or processing of personal data and the potential risk implications.

(ii) **Stage 2: Formulate a DPIA plan**

Upon determining the need, organisations can continue to formulate a DPIA plan which covers a description of the project, scope of data protection assessment and risk criteria, types of stakeholders from whom input is required and setting a timeline to complete the DPIA exercise.

(iii) **Stage 3: Identify Data and Data Flows**

At this stage, relevant information and documentation of the project should be collected such as contracts with service providers and other third parties, internal reports, project plan and technical specifications of the system. Organisations can establish the flows of personal data of the project through a Data Inventory Map and record how data is managed across the data life cycle.

(iv) **Stage 4: Identify and Assess Risks**

Organisations should identify and evaluate the data protection risks against the requirements of the PDPO and any relevant industry standards. Other considerations include the severity of impact or adverse consequences on individuals that may arise from its data processing activities.

(v) **Stage 5: Identify Measures to Mitigate Identified Risks**

Organisations would need to determine the measures to be implemented to address risks and develop a mitigation action plan. The plan can include the recommended measures and options to mitigate the identified risks, the responsible stakeholders for its implementation, the implementation timeline and applicable legal or regulatory requirements.

(vi) **Stage 6: Implement and Monitor Action Plan**

At the end of the assessment, a DPIA report should be written and documented for future reference of its data protection recommendations and rationales, as well as serve as an internal record of how the organisation took steps to consider the management of risks for the system or process. Any changes to the project may require another review in order to address any new data protection risks or gaps.

(b) Generally, a DPIA can be implemented by the project manager or departmental head which is primarily responsible for the management of personal data involved in the system, with the assistance of the DPO. They are typically referred to as the DPIA Lead.

(c) The DPO should ensure that the recommendations in the DPIA report will be able to streamline its processes to adhere to the organisation's data protection policies and facilitate in the compliance to the PDPO.

Illustration of mapping data flows through Data Inventory when conducting a DPIA
(Reference is made to 4.1.2(a) and 4.1.3(a)(iii))

Organisation J is a leisure and recreational club which collects and processes personal data of its members through a registration form on its website. It has engaged a service provider to develop a mobile application for existing members to book a slot to join a recreational class.

The Business Project Manager is tasked as the DPIA Lead and identifies the relevant stakeholders for assessing the above process to be the IT Manager, Sales Manager and Legal Manager. The DPIA Lead involves the DPO in the mapping exercise which captures the process of the data flows of new members booking a recreational class. Collectively, they put together a Data Inventory map and are recorded as follows:

Data Inventory Map for Membership Database (Note: Illustrative purposes only)					
Data Owner	**Data Subject**	**Types of Personal Data**	**Purposes of Collection and Use**	**Legal Basis**	**Time and manner of collection**
Recreational Club	New Member1	Full Name, Date of Birth, Contact No	Use of facilities	Consent	Upon submitting the Online Registration Form
External Recipients	**Time and manner of collection**	**Storage Location (Physical)**	**Storage Location (Electronic)**	**Security Measures**	
Online Booking App	Upon booking a recreational class	N/A	Cloud	Access Controls, Encryption. Data Loss Prevention	

The DPO assists in ensuring the Data Protection Policy is up to date to include information on how the organisations process personal data of its members and ensures members are notified through a readily accessible tab on the mobile application. Furthermore, the DPO assists in ensuring that proper security measures are in place when the service provider processes personal data on behalf of the Recreational Club.

4.2. The abovementioned tools may be useful for the organisation's assessment of its systems and processes. It is thereby essential to appoint a DPO that can assist in facilitating the compliance to the PDPO when organisations carry out such assessments.

4.3. In general, organisations should consider to adopt any such tools that fits its operations and establish its own Data Protection Management Programme ("**DPMP**") within the organisation in order to ensure that it develops and implements appropriate measures. [5]

[END]

[5] For more information, refer to AITI's Guide on Developing a Data Protection Management Programme.