مركز حماية البيانات الشخصية
PDPC
Personal Data Protection Center

DATA PROTECTION OFFICER GUIDELINES

Personal Data Protection Center

Version 1.1. - 26 January 2026

Disclaimer

The Personal Data Protection Center reserves the right to amend, update, or replace any of the content, templates, or interpretive or regulatory guidelines published on this portal, in whole or in part, at any time, within the scope of its mandates. The information, templates, or guidelines published shall not be deemed binding administrative or regulatory decisions, and no legal, contractual, or tortious obligation or liability shall arise on the part of the Center as a result of their publication, amendment, or reliance thereon. Furthermore, they do not replace or negate the obligation to comply with the provisions of the Personal Data Protection Law as enacted by Law No. 151 of the year 2020 and the Executive Regulations issued by Decision No. 816 of 2025.

Introduction

The data protection officer (DPO) is a function newly established by the Personal Data Protection Law (PDPL). A DPO is a natural person responsible for assisting and overseeing data users in complying with the data protection regulatory framework.

Juridical persons acting as data users must appoint a DPO irrespective of the scale of their processing activities. Natural persons acting as data users may either appoint a DPO or personally assume the obligations associated with this role.

This guideline sets out:

1. The DPO's key responsibilities;
2. The DPO's registration;
3. The DPO's appointment;
4. Data users' obligations towards the DPO; and
5. The DPO's termination of appointment and replacement.

1. The Key Responsibilities of the DPO

The DPO has three main responsibilities:

- Overseeing the data user's compliance with personal data protection obligations;
- Being a point of contact for data subjects' requests and complaints; and
- Being a point of contact with the Personal Data Protection Centre (PDPC).

1.1. Overseeing the Data User's Compliance with Personal Data Protection Obligations

A DPO has the obligation of overseeing and ensuring the data user's compliance with personal data protection obligations.

Such a role includes:

- Assisting data users in the development and implementation of a privacy program;
- Ensuring the effective implementation of PDPC decisions and guidelines;
- Advising the data user on how to comply with personal data protection obligations;
- Overseeing the maintenance, accuracy, and regular updating of the record of processing activities (ROPA);
- Reviewing and advising on the organisation's privacy policies;
- Supporting the delivery of data protection training and awareness programs to the data user's employees;
- Reviewing data protection risk assessments (e.g., DPIAs, LIAs);
- Advising the data user on the determination of appropriate technical and organisational data protection measures;
- Advising the data user on appropriate personal data breach management measures; and
- Ensuring effective procedures and measures are in place to enable data subject rights, and that data subject complaints are duly received, managed, and addressed.

For more information on personal data protection obligations, please refer to the Data Users Guideline.

1.2. Point of Contact for Data Subjects' Requests and Complaints

The DPO acts as the primary contact point for all data subjects' requests and complaints. The DPO must ensure that there are appropriate processes in place to handle any inquiry, request, or

complaint regarding the processing of personal data, and must oversee that they are addressed within the timeframe determined by the PDPL.

This does not imply that the DPO must personally execute data subject requests themselves, but rather ensure the process is properly handled and managed (e.g., ensuring the request is forwarded to the relevant department and that appropriate actions are taken to fulfil it).

The DPO's contact details must be made available, both publicly and internally within the entity, to ensure both internal and external data subjects can easily and directly contact them.

1.3. Point of Contact with the PDPC

The DPO serves as the designated point of contact for all communications to the PDPC concerning the data user's processing activities. Additionally, the DPO must:

- Notify the PDPC of personal data breaches within the legally required timeframe;
- Submit annual reports to the PDPC on the personal data protection compliance status of the data user, and upon the request of the PDPC; and
- In the case of DPO replacement, submit reports to the PDPC on the data user's personal data protection compliance status within 15 days of the replacement. This is to be done by the newly appointed DPO.

2. The Registration of the DPO

The PDPC has established an electronic registry, known as the DPO Registry, in which DPOs must be registered in order to be recognised as such.

2.1. Qualification Criteria

While no specific professional background is required, the DPO must meet the following qualification criteria to be eligible for registration:

- Possession of an academic degree or professional credentials:
    - An academic degree, preferably in law, computer science, or a related field.
    - Professional credentials in the field of data protection (e.g., IAPP certifications).
- Successful completion of the PDPC exam. *For more information on DPO exams, please refer to the DPO Categories Guideline.*
- Having no convictions involving dishonesty or breach of trust.

2.2. Registration Application

The registration application shall be submitted personally by the DPO applicant through the PDPC's electronic portal.

Applications to register require submitting the following:

- A copy of the national ID for Egyptians or passport for foreigners;
- A recent personal photo of the applicant;
- Evidence of meeting the qualification criteria;
- A copy of the applicant's criminal record. For foreign applicants, the record must be duly certified by the relevant authorities; and
- Payment of application fees.

2.3. PDPC Assessment of Application

The PDPC will assess applications and conduct DPO registration in accordance with the following process:

- If all required information and documents are submitted in the initial application, the PDPC will determine the application within thirty (30) working days from the date of submission.
- If the PDPC considers that additional documents, information, or actions are required, the PDPC will formally notify the applicant and specify a deadline for completing the application. Once the application is completed, the PDPC will determine the application within fifteen (15) days from the completion date.
- Where the application is accepted, the applicant must pay the registration fee to be listed on the DPO Registry.
- Upon registration, the DPO will receive a unique identification number referred to as the "DPO Code".

For more information on DPO qualification criteria, DPO registration, as well as reassessment and renewal of DPO certification, please refer to the DPO Categories Guideline.

3. The Appointment of the DPO

3.1. Appointment Obligation

Juridical persons acting as data users must appoint a DPO irrespective of the scale of their processing activities. Natural persons acting as data users may either appoint a DPO or personally

assume the obligations associated with this role. In all cases, such appointment must be in accordance with the following conditions:

- The DPO must be registered on the PDPC's DPO Registry;
- The DPO's category must correspond to the data user's processing activities; and
- A declaration of appointment signed by both parties must be submitted to the PDPC.

For more information on DPO categories, please refer to the DPO Categories Guideline.

3.2. The DPO Position in the Organisational Chart

The DPO may either be an internal employee or an external service provider.

Furthermore, the same DPO may be appointed by two or more data users, and is referred to as a "shared DPO". Such appointment may be made by unrelated or intra-group entities, provided that the following conditions are met:

- The appointment complies with the conditions set out in Section 3.1.;
- Only in case of unrelated entities, each data user has formally authorised the DPO to undertake such responsibilities through the PDPC electronic portal;
- No conflict of interest arises from the shared DPO appointments. Any conflict of interest— whether existing at the time of appointment or arising thereafter—must be promptly reported to the PDPC, which will assess the situation and either approve or reject the appointments; and
- The PDPC has approved the shared DPO appointments.

> **Note:**
>
> The shared DPO must ensure that their record-keeping is appropriately segregated and organised for each data user. This is essential for them to perform their duties independently and to enable the PDPC to conduct proper reviews as may be needed.

4. Data Users' Obligations Towards the DPO

To ensure the DPO can perform their duties effectively, data users must:

- Ensure the timely and appropriate involvement of the DPO in all matters related to personal data protection.
- Allow the DPO to exercise their role with full independence and refrain from any undue influence. This means a DPO can neither be instructed, penalised, nor threatened for performing their duties. Such an obligation must be included in the contract governing the DPO-data user relationship.

- Provide necessary support for the DPO. This includes providing the DPO with all required resources, as well as complete and accurate information, within a reasonable timeframe that enables the DPO to perform their duties effectively.
- Ensure the existence of appropriate communication channels that enable the DPO to perform their duties effectively and to report to management and relevant stakeholders.
- Ensure that no conflict of interest affects the DPO's independence. If the DPO occupies another role within the same entity, the data user must ensure that the exercise of any such function does not compromise the DPO's independence or ability to perform their duties in full neutrality.

5. Termination of Appointment and Replacement

5.1. Termination by the Data User or the DPO

Before the effective date of a DPO termination, the legal representative of the data user must ensure DPO replacement is done in accordance with the aforementioned appointment conditions and process.

Furthermore, the legal representative must notify the PDPC via the electronic portal at least fifteen (15) days prior to the termination's effective date, specifying:

- The reason for termination (e.g., end of contract without renewal, resignation, dismissal, incapacitation, or death);
- The registration code of the newly appointed DPO; and
- The duration of the mandate of the newly appointed DPO, in case such mandate is temporary.

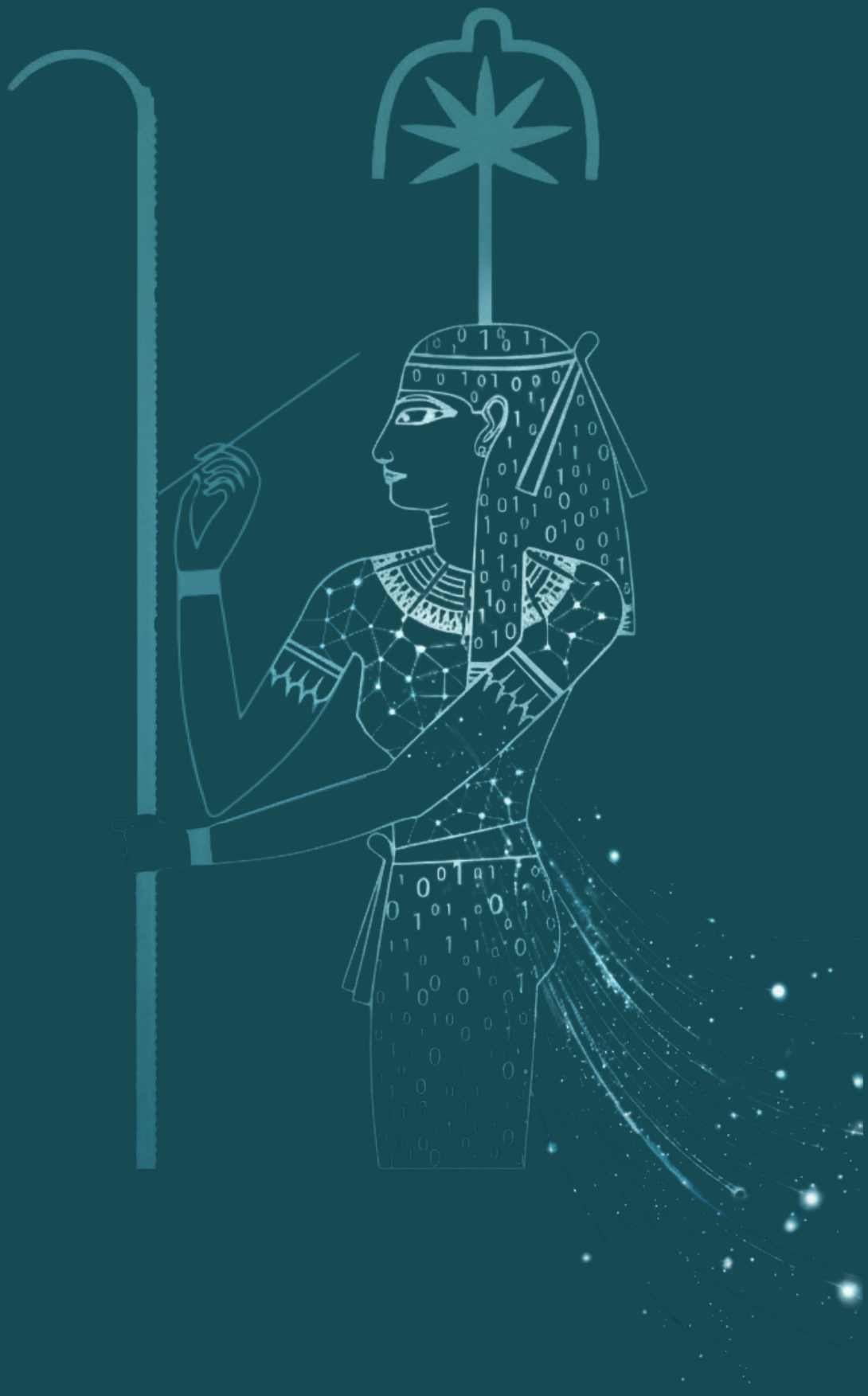
5.2. Termination by the PDPC

If the PDPC discovers a DPO has breached any of the registration requirements, (e.g., forging a document) such DPO will be removed from the DPO Registry. The PDPC will then notify the data user of the DPO's removal and require the data user to dismiss the DPO immediately.

> **Note:**
>
> Where there are unforeseen circumstances preventing the legal representative from complying with the aforementioned obligations related to the DPO replacement (e.g., due to the death of the DPO), they must:
>
> - Promptly notify the PDPC, providing a detailed justification and supporting documentation;

- Promptly appoint a new DPO—whether a temporary DPO or a regular-term DPO—in accordance with the aforementioned appointment conditions and process; and
- Where a temporary DPO is appointed, appoint a regular-term DPO and notify the PDPC, in accordance with the appointment conditions, within thirty (30) days from the awareness of the unforeseen circumstances.

Tip: **It is more practical to create generic contact details for DPOs (such as a generic email like dpo@company.com) to ensure uninterrupted communication in case of DPO replacement.**



@pdpceg

info@pdpc.gov.eg