مركز حماية البيانات الشخصية
PDPC
Personal Data Protection Center

RECORD OF PROCESSING ACTIVITIES 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

Pursuant to the Personal Data Protection Law (PDPL), all processing activities must be documented by data users in a record of processing activities (RoPA). The PDPL sets different requirements for both controller-related-activities (Article 4.9) and processor-related-activities (Article 5.9).

This guideline sets out:

1. The RoPA concept;
2. Steps to develop a RoPA; and
3. RoPA structure and content.

1. The RoPA Concept

A RoPA is a structured record capturing key information on all personal data processing activities.

Beyond the explicit obligation on all data users to maintain a RoPA, such record constitutes the first step towards achieving and demonstrating compliance with most obligations under the PDPL.

Serving as a core data governance tool, the RoPA enables data users to gain a clear understanding of their processing activities, including their context, nature, and lifecycle. Without such visibility, data users cannot effectively identify or implement the appropriate measures for compliance with the PDPL requirements.

The RoPA must be accurate, complete, updated, and made available to the Personal Data Protection Centre (PDPC) upon request.

2. Steps to Develop a RoPA

The following steps outline a structured approach recommended by the PDPC to ensure the accuracy, completeness, and consistency of the information recorded in the RoPA.

> **Note:**
>
> Data users must ensure the involvement of the data protection officer (DPO) as they are responsible for overseeing the preparation process and ensuring that the RoPA is complete and accurate.

a. Conduct an Asset Inventory

Begin by identifying all systems, applications, databases, and repositories that process and store the entity's data, including those located on external devices or operated by third parties (e.g., devices used by consultants). Engage relevant departments, such as IT and finance, to ensure effective identification of all data assets.

b. Consider Data Discovery Tools

Where feasible, use data discovery tools to automatically locate all data across systems. These tools can enhance accuracy, minimise manual effort, and ensure that no data is overlooked.

c. Prepare the Interview Framework

Develop a structured questionnaire to collect relevant information from data owners and relevant stakeholders, ensuring that all RoPA requirements are addressed consistently and comprehensively across all departments.

d. Conduct Interviews with Data Owners

Data owners are the individuals accountable for specific sets of data within the entity. Engage directly with them to collect all mandatory information on each processing activity and fill it in the RoPA template.

e. Classify Personal Data

The RoPA requires the identification of non-sensitive personal data, sensitive personal data, and children's personal data. Moreover, data classification is a crucial exercise that data users must conduct to ensure the proper security of personal data.

f. Ensure Regular Review and Updates

Establish a process for periodically reviewing and updating the RoPA, especially when new processing activities are introduced or existing ones are modified, to ensure it remains current and accurate.

3. RoPA Structure and Content

The RoPA is best presented in a table format, where each row represents distinct processing activities, while columns capture the key information describing the associated processing activity. The information required in a controller-related-activities RoPA differs from that required in a processor-related-activities RoPA, meaning that data users must keep separate RoPAs.

The PDPC has developed two RoPA templates: one for controllers and controllers/processors, and another for processors. Data users shall complete the template that corresponds to their role in each processing activity.

Each template is accompanied by hypothetical examples to illustrate how the fields may be completed for pure guidance purposes. *To download the template, please refer to RoPA Templates.*

Data users remain free to utilise any alternative template, provided it captures all information mandated by the data protection regulatory framework.

The following outlines the mandatory information required for each RoPA type:

3.1 The Controller-Related-Activities RoPA

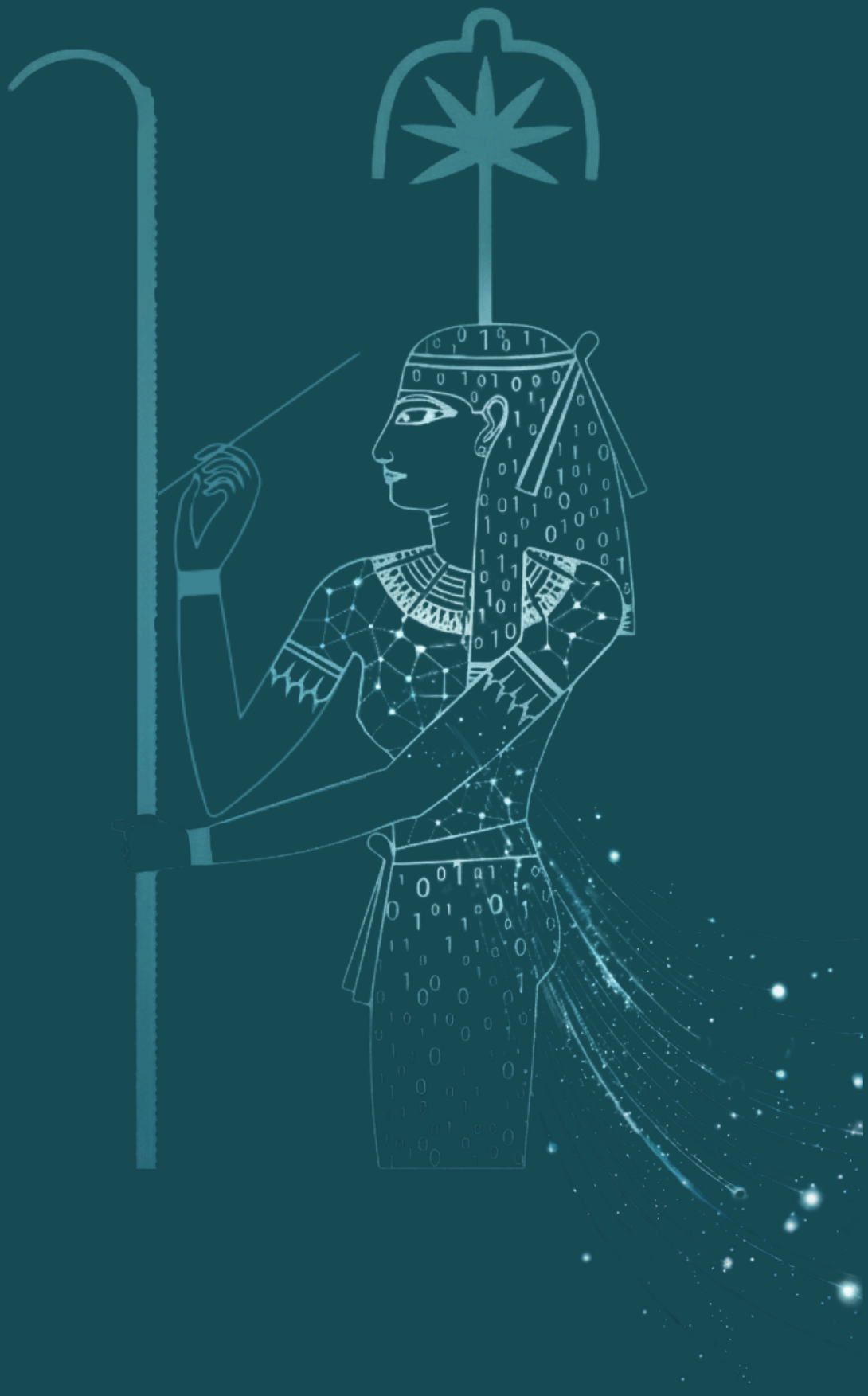
- The type of the data user: controller or processor.
- The name and contact details of the data user.
- The name and contact details of the DPO.
- The name and contact details of the data user's legal representative.

- The purpose(s) of processing activity.
- The sub-purpose(s) of processing, if available.
- The category(ies) of data subjects.
- The data owner.
- The categories of personal data, including its classification as non-sensitive data, sensitive data, and children's data.
- The data collection source.
- The lawful basis.
- Legitimate interest assessment (LIA) link, if applicable.
- The data hosting environment: on-premises or on cloud.
- The data hosting location: inside or outside the Arab Republic of Egypt.
- The retention period or the criteria of determining it.
- The data disposal measure(s).
- The organisational roles with access to the data.
- The implemented technical security measures.
- The implemented organisational security measures.
- Data protection impact assessment (DPIA) link, if applicable.
- The recipient(s) or category(ies) of recipient(s).
- The legal characterisation of the recipient(s).
- Data protection agreement link (e.g., data processing agreement, data sharing agreement).
- The foreign country(ies) data is transferred to.
- The basis of cross-border transfer.
- The implemented security measures for cross-border transfer.
- Transfer impact assessment (TIA) link, if applicable.

3.2 The Processor-Related-Activities RoPA

- The type of the data user: controller or processor.
- The name and contact details of the data user.
- The name and contact details of the DPO.
- The name and contact details of the data user's legal representative.
- The category(ies) of processing activity.

- The contact details of the controller and the controller's legal representative and DPO.
- Data processing agreement link.
- The retention period and instructions specified by the controller.
- The data disposal measure(s).
- The implemented technical security measures.
- The implemented organisational security measures.
- The sub-processor or category(ies) of sub-processor(s).
- Sub-processor agreement link.
- The foreign country(ies) data is transferred to.
- The legal basis of cross-border transfer.
- The implemented security measures for cross-border transfer.



@pdpceg

info@pdpc.gov.eg