مركز حماية البيانات الشخصية
PDPC
Personal Data Protection Center

DATA USERS 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 2
1. The Concept of Data Users 3
1.1. The Distinction Between Controllers and Processors 3
1.2. Controllers/Processors 6
2. The Relationship Between Data Users 6
3. Legal Obligations 7
3.1. Appointing a Data Protection Officer (DPO) 7
3.2. Obtaining the Necessary Licenses and Permits 7
3.3. Maintaining a Record of Processing Activities (RoPA) 8
3.4. Processing Personal Data in Accordance with Data Protection Principles 8
3.5. Enabling Data Subjects' Rights 9
3.6. Complying with Sensitive Personal Data Obligations 9
3.7. Conducting the Necessary Data Protection Risk Assessments 9
3.8. Complying with Breach Notification Obligations 10
3.9. Complying with Electronic Direct Marketing Obligations 10
3.10. Appointing a Representative in Egypt 10
3.11. Cross-Border Data Transfer Obligations 11
3.12. Data Protection Clauses 11
3.13. Following the Controller's Instructions 11
3.14. Cooperating with the PDPC 11

Introduction

Controllers and processors are the primary subjects of obligations under the Personal Data Protection Law (PDPL), with each assuming distinct roles and responsibilities in relation to the processing activity in question. Accordingly, understanding these differences is crucial to ensuring effective compliance with the data protection regulatory framework.

This guideline sets out:

1. The concept of data users;
2. The relationship between data users; and
3. Their respective legal obligations under the PDPL.

1. The Concept of Data Users

The term "data user" is a general designation that includes controllers, processors, and controllers/processors.

	Controller	Processor
PDPL Definition	Any natural or juridical person who— by virtue of their work or by nature of their activity — has the right to obtain and control personal data, as well as to determine the means, techniques, and criteria governing the retention or processing of such data, in accordance with the specified purpose or their activity.	Any natural or juridical person who — by nature of their activity — processes personal data for their own interest, or for the interest of the controller in accordance with the terms agreed upon and the instructions provided by the controller.
Examples of natural persons	• Doctors • Lawyers • Accountants	• IT consultants • Freelance data entry specialists • Independent marketing specialists
Examples of juridical persons	• Government authorities • Hospitals • Corporations • NGOs	• Cloud service providers • Payroll companies • Call centre service providers • Marketing agencies

Note:

Individuals collecting or processing personal data solely for personal purposes are excluded from the scope of the PDPL (e.g., an individual maintaining contact details of friends and family on their phone).

1.1. The Distinction Between Controllers and Processors

Being a controller or processor is not a blanket characterisation of the entity, but rather reflects the role they assume in a specific processing activity, and this characterisation may even vary at different stages of the processing activity lifecycle.

Accordingly, data users must not rely on assumptions, general titles, or contractual descriptions. Instead, they must conduct a case-by-case assessment, based on their factual roles

in each processing activity, to determine the appropriate legal characterisation and understand the corresponding legal obligations.

> **Example:**
>
> Company A is a software development company that processes personal data on behalf of Company B and strictly in accordance with the instructions of Company B. In this processing activity, Company A acts as a processor.
>
> In another context, Company A determines the purpose and means of processing their employees' personal data and carries out the processing. In this processing activity, Company A acts as a controller.

a. Controllers

To identify a controller, the decisive criterion is whether an entity is exercising control and decision-making authority over the purpose(s) and means of the personal data processing activities.

The purpose(s) of the processing: "the why"

The purpose refers to the reason or objective for which personal data is collected or processed, defining the scope and limitations of the processing activity.

Accordingly, an entity that determines the purpose of a processing activity is regarded as a controller in respect of that activity, irrespective of the contractual designation attributed to them.

The means of the processing: "the how"

The means refer to how the purpose of processing will be achieved by determining the conditions under which personal data is collected, stored, used, secured, transferred, disposed, etc.

There are essential and non-essential means. Determining the essential means is reserved for controllers, while non-essential means can be determined by either a controller or a processor, without altering the processor's characterisation or rendering them a controller.

- **Essential means:** Related to the scope and the fundamental aspects of the processing activity. Examples include:
  - The categories of data subjects involved;
  - The personal data processed;
  - The retention periods of personal data; and
  - The recipient(s) of personal data.

- **Non-essential means:** Related to the practical and technical aspects of the processing activity. Examples include:
  - The system and hardware used to carry out the processing;
  - The security measures implemented to protect the personal data;
  - Internal workflow and distributions of tasks on employees; and
  - Details of storage logistics.

Example 1:

A retailer company creates and maintains a fan page on a social media platform. The platform places cookies on visitors' devices to track their browsing behavior and provides the company with anonymised statistical insights about page visitors.

The company sets parameters defining the target audience and objectives, influencing how visitor statistics are generated, and which personal data categories are processed.

Even without directly accessing personal data, the company is considered a joint controller because it influences the purposes and means of processing and enables the platform to place cookies on visitors' devices.

Example 2:

A payroll service provider determines the software tools, and internal workflow steps used to calculate and issue salaries on behalf of the controller.

Despite determining these details, the payroll service provider remains a processor, because these operational means are non-essential means and can be determined by the processor without exceeding its role.

b. Processors

To identify a processor, the decisive criterion is whether an entity processes personal data on behalf of a controller, in accordance with the agreed terms and documented instructions.

Example:

Company A—a customer support service provider—is engaged by Company B to handle customer inquiries on their behalf. In performing these services, Company A processes the personal data of Company B's customers strictly in accordance with Company B's documented instructions and the terms of their agreement. In this context, Company A acts as a processor.

1.2. Controllers/Processors

A controller/processor refers to any entity that both determines the purposes and means of a processing activity and directly carries out that processing activity, whether wholly or partially.

In other words, whenever an entity processes personal data for their own benefit, it acquires the status of controller/processor in respect of that activity. Such an entity, therefore, assumes the combined obligations of controllers and processors under the PDPL.

It should be noted that under the PDPL, the term *"processing"* is broadly defined to include activities such as collecting personal data. Since most controllers engage in processing when collecting and using personal data, almost all controllers qualify as controller/processor.

> **Example:**
>
> Company A collects the personal data of their own customers and processes it for delivery and order-fulfilment purposes. In such a case, Company A is regarded as a controller/processor and should assume the obligations associated with both roles.

2. The Relationship Between Data Users

Relationships between data users may give rise to complex legal and operational considerations, including potential overlapping responsibilities.

Therefore, to mitigate the risk of incurring liabilities for another party's non-compliance, data users are advised to clearly define their respective data protection roles and responsibilities in a written agreement annexed to their main agreement.

Such agreements must be consistent with the data protection regulatory framework and other applicable laws and regulations, and may include:

- Scope and limitations, inter alia, the purpose(s) of the processing activity and the categories of personal data;
- Data protection undertakings specifying each party's obligations;
- Audit and inspection rights;
- Assistance with data subject requests;
- Security measures to be implemented;
- Procedures for data breach notifications;
- Procedures of data return and disposal;
- Provisions governing the instructions and communications; and
- Approvals and notifications required for engaging a sub-processor.

3. Legal Obligations

Data users must observe the following and comply with the data protection obligations applicable to their role and processing activities:

1. Appointing a data protection officer (DPO);
2. Obtaining the necessary licenses and permits;
3. Maintaining a record of processing activities (RoPA);
4. Processing personal data in accordance with data protection principles;
5. Enabling data subjects' rights;
6. Complying with sensitive personal data obligations;
7. Conducting the necessary data protection risk assessments;
8. Complying with breach notification obligations;
9. Complying with electronic direct marketing obligations;
10. Appointing a representative in Egypt;
11. Cross-border data transfer obligations;
12. Data protection clauses;
13. Following the controller's instructions; and
14. Cooperating with the PDPC.

3.1. Appointing a Data Protection Officer (DPO)

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.

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

3.2. Obtaining the Necessary Licenses and Permits

Data users must obtain a controller, processor, or controller/processor license or permit from the PDPC in order to process personal data. Additionally, depending on the nature of their activities, they must obtain a supplementary license or permit for electronic direct marketing, video surveillance systems, or cross-border data transfers. In this regard, they must:

- Complete the license and permit compliance checklist;
- Submit the necessary documentation, if needed;
- Respond to the queries of the PDPC during the application process;
- Pay the applicable fees; and
- Comply with terms and conditions governing the issued licenses and/or permits.

For more information on licenses and permits, please refer to the Licenses and Permits Guideline.

3.3. Maintaining a Record of Processing Activities (RoPA)

A RoPA is a structured record capturing key information on all personal data processing activities conducted by data users. RoPA must be maintained accurately, kept up to date, and made available to the PDPC upon request.

For more information on the RoPA and its requirements, please refer to the RoPA Guideline. To access the RoPA templates of the PDPC, please refer to the RoPA Templates.

3.4. Processing Personal Data in Accordance with Data Protection Principles

Data users must adhere to the fundamental data protection principles set forth by the PDPL.

- **Lawfulness:** Processing personal data must rely on at least one lawful basis and must be conducted in compliance with applicable laws and regulations.
- **Fairness:** Processing personal data must align with data subjects' reasonable expectations and ensure that they are not subjected to unjustified harm.
- **Transparency:** Personal data must be processed in a manner that is clear, open, and honest towards the data subject.
- **Purpose limitation:** Processing personal data must be for specified, explicit, and legitimate purposes, and any further processing must be compatible with the original purpose.
- **minimisation:** Processing and collection of personal data must be limited only to the extent that is relevant, adequate, and necessary for the intended purpose(s) of the processing activity.
- **Data accuracy:** All reasonable steps must be taken to ensure that personal data is accurate, complete, and kept up to date in accordance with the purpose(s) of the processing activity.
- **Storage limitation:** Processing personal data must be for specified, explicit, and legitimate purposes, and any further processing must be compatible with the original purpose.
- **Data security:** Personal data must be secured and protected throughout its entire lifecycle against any unlawful or unauthorised processing, access, alteration, damage, loss, or destruction.
- **Accountability:** Processing personal data must be for specified, explicit, and legitimate purposes, and any further processing must be compatible with the original purpose.

For more information on data protection principles, please refer to the Data Protection Principles Guideline.

3.5. Enabling Data Subjects' Rights

Data users must enable the following data subject rights within the required conditions and timeframes:

- **The right to be informed:** the data subject's right to be proactively and effectively provided with adequate information about the processing of their personal data. *For more information about the right to be informed, please refer to the Privacy Notice Guideline.*
- **The right to be notified in case of data breach:** the data subject's right to be notified, in a timely manner, of any data breach affecting their personal data.
- **The right of access:** the data subject's right to obtain confirmation as to whether their personal data is being processed and, where applicable, to receive a copy of such data and/or the requested information about the processing activity.
- **The right to withdraw consent:** the data subject's right to freely revoke their previous consent at any time through a clear, simple, accessible, and cost-free mechanism.
- **The right to erasure "Right to be forgotten":** the data subject's right to have their personal data erased from data users' records.
- **The right to rectification:** the data subject's right to have their personal data corrected or updated.
- **The right to object:** the data subject's right to object to and require the cessation of the processing of their personal data.
- **The right to restriction of processing:** the data subject's right to temporarily restrict the processing of their personal data solely within the storage scope.
- **The right to data portability:** the data subject's right to have their personal data transferred to another controller in a structured, commonly used, and machine-readable format.

3.6. Complying with Sensitive Personal Data Obligations

Data users must properly classify personal data to identify any categories of sensitive personal data and ensure enhanced protection of such data. This includes complying with the appropriate consent requirements and implementing appropriate technical and organisational measures to safeguard such data.

For more information about consent requirements when processing sensitive data, please refer to the Data Subject's Consent Guideline.

3.7. Conducting the Necessary Data Protection Risk Assessments

Data protection risk assessments (e.g., DPIA and LIAs) are processes by which the data user identifies, assesses, and mitigates data protection risks. Such assessments must be properly documented and made available to the PDPC upon request.

3.8. Complying with Breach Notification Obligations

Data users must:

- Implement appropriate technical and organisational measures to detect, manage, and remediate personal data breaches;
- Notify the PDPC of any personal data breach, with all mandatory information, within seventy-two (72) hours of becoming aware of the breach, or immediately if the breach concerns a matter of national security;
- Notify data subjects of any personal data breach concerning their personal data, with all mandatory information, within three (3) working days following the notification to the PDPC; and
- Maintain a complete, accurate, and up-to-date personal data breach register.

3.9. Complying with Electronic Direct Marketing Obligations

Data users engaged in electronic direct marketing (EDM) must comply with the following obligations, depending on their respective marketing roles:

- Obtain the necessary EDM license or permit before initiating any EDM communications (EDMCs);
- Obtain the data subject's valid consent prior to sending any EDMCs;
- Honour opt out requests in a timely manner;
- Maintain an updated and accurate record of all opt-out requests;
- Refrain from disclosing data subjects' contact information to any unauthorised entity;
- Ensure EDMCs include all information mandated by the PDPL; and
- Maintain electronic records evidencing the data subject's consent, including any amendments or consent withdrawals. These records must be retained for a period of three (3) years from the date of the last EDMC sent to the data subject.

For more information about EDM obligations, please refer to the EDM Guideline.

3.10. Appointing a Representative in Egypt

Data users located outside the Arab Republic of Egypt, without having a branch or representative office within the Egyptian borders, must appoint a representative within Egypt. For juridical persons, the representative may be a company branch, or an office authorised to act on their behalf or represent them. For natural persons, the legal representative must reside in Egypt.

In all cases, the appointed representative shall be officially registered by the PDPC for the duration of the applicable licence or permit.

3.11. Cross-Border Data Transfer Obligations

When engaging in a cross-border data transfer, data users must:

- Obtain a cross-border data transfer permit or licence, where applicable;
- Ensure all cross-border data transfers rely on an appropriate legal basis; and
- Conduct an accurate, complete and documented Transfer Impact Assessment (TIA), where applicable.

3.12. Data Protection Clauses

Data users are advised to clearly define their respective data protection roles and responsibilities in a written agreement annexed to their main agreement, to ensure compliance with the data protection regulatory framework.

3.13. Following the Controller's Instructions

Processors must process personal data strictly in accordance with the controllers' instructions, unless such instructions violate the applicable laws or regulations. In the latter case, processors must promptly inform controllers accordingly.

3.14. Cooperating with the PDPC

Data users must cooperate diligently, promptly and in good faith with the PDPC, inter alia:

- Responding to the PDPC queries;
- Providing the PDPC with the required documents and information; and
- Allowing the inspectors of the PDPC to access the electronic records to verify compliance with data protection regulatory framework.

@pdpceg

info@pdpc.gov. eg