مركز حماية البيانات الشخصية
PDPC
Personal Data Protection Center

LAWFUL BASES OF PROCESSING 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 lawfulness principle stands at the core of the Personal Data Protection Law (PDPL), ensuring that personal data is collected, processed, retained, and disclosed only when justified by valid legal reasons. As such, the lawfulness principle maintains a fair balance between enabling business needs and safeguarding data subjects against any unjustified interference with their privacy.

To this end, all processing activities must rely on at least one of the six lawful bases enumerated under Article 6 of the PDPL. Data Users must—prior to initiating any processing activity—determine the applicable lawful basis, conduct the necessary assessments to ensure the validity of the basis, and maintain appropriate documentation demonstrating compliance.

This guideline sets out the lawful bases of processing personal data:

1. Data subject's consent;
2. Fulfilment of a contractual obligation;
3. Fulfilment of a legal obligation;
4. Legitimate interest;
5. Claim or defence of a legal right; or
6. Execution of court judgments or orders from competent investigative authorities.

1. Data Subject's Consent

To be considered valid, the data subject's consent must always be personal, explicit, informed, specific, and freely given.

Moreover, processing sensitive personal data based on consent must meet stricter additional conditions.

1.1. General Conditions

- **Personal:** Consent must be provided directly by the data subject or by their authorised legal representative.
- **Explicit:** Consent must be clear and unequivocal, leaving no doubt as to the data subject's intention to authorise the processing of their personal data.
- **Informed:** The data subject must be adequately informed about the processing of their personal data, including at least:
    1. The controller's identity;
    2. The purpose(s) of the processing;
    3. The categories of data that will be processed; and
    4. The right to withdraw consent at any time.
- **Specific:** The information provided to the data subject regarding the processing activity must be clearly defined, and neither vague nor bundled. Moreover, the consent remains valid only for the specific information communicated to the data subject.
- **Freely given:** The data subject must have a genuine choice to accept or refuse the processing of their data without feeling coerced or compelled to do so.

1.2. Additional Conditions for Sensitive Personal Data

As the processing of sensitive personal data may present high risks to data subjects' rights and freedoms, additional conditions must be satisfied for the consent to be considered valid.

> **Note:**
>
> Sensitive data, as defined under Article 1 of the PDPL, consists of the following:
>
> - *Genetic data;*
> - *Biometric data;*
> - *Health data;*
> - *Financial data;*
> - *Religious beliefs;*
> - *Political opinions;*
> - *Security data; and*
> - *Children's data.*

- **Written:** Consent for all categories of sensitive personal data must be in writing, whether in paper form or through electronic means.
- **Legal Guardian's Consent:** The processing of children's personal data requires consent from the child's legal guardian, considering the following:
    - For children under the age of 15, consent must be provided only by the guardian.
    - For children over the age of 15, the consent can be provided by either the child or the guardian, as long as the guardian is aware of the child's consent.

For more information on the data subject's consent, please refer to the Data Subject's Consent Guideline.

2. Fulfilment of a Contractual Obligation

This lawful basis applies where the processing of personal data is required for the performance of a contract to which the data subject is a party, or to take steps to enter into such a contract (e.g., filling in forms, requesting quotations, etc…).

For reliance on this basis to be valid, the processing must be strictly necessary to execute or conclude the contract, in a manner that the contract could not reasonably be performed without the required personal data.

> **Example 1:**
>
> A social media platform (SMP) collects users' data, including browsing behaviour on their own- and third-party platforms to personalise the content displayed. The SMP claims to rely on fulfilment of contractual obligation as a lawful basis, asserting that users accept their general terms of use mandated to access their services.
>
> This processing activity is not lawful, as the collection of such data and personalising the content is not objectively necessary to fulfil the contract's main subject-matter (providing the social networking service) which could be delivered without such processing.

> **Example 2:**
>
> An online retailer collects gender data to personalise order confirmation emails by addressing customers as "Dear Sir" or "Dear Madam". The retailer claims to rely on fulfilment of contractual obligation as a lawful basis, asserting that personalised greetings are part of their brand and show respect to customers.
>
> This collection is not lawful, as personalising emails by gender is not objectively necessary to fulfil the contract's main subject-matter (selling products and confirming orders), particularly when less data-driven alternatives, such as "Dear Customer," could achieve the same purpose.

Example 3:

An insurance company collects a strict amount of personal data from prospective customers to assess eligibility and determine policy terms before entering into a contract.

This processing activity is lawful, as the data collection is strictly necessary to take steps at the request of the data subject for issuing an appropriate insurance policy.

3. Fulfilment of a Legal Obligation

To be considered valid, the processing activity must be strictly necessary to comply with a legal obligation imposed by applicable laws and regulations.

Example 1:

A financial institution retains customers' personal data for five years from the date of account closure to comply with the obligation prescribed under Article 9 of the Anti-Money Laundering Law, as enacted by Law No. 80 of the year 2002. Such processing activity is deemed lawful under the fulfilment of legal obligation basis.

Example 2:

A hotel is collecting customers' personal data, such as their names and nationalities, to comply with the obligation prescribed under Article 13 of Prime Minister's Decree No. 705 of the year 2023. Such processing activity is deemed lawful under the fulfilment of legal obligation basis.

4. Legitimate Interest

Legitimate interest can be perceived as a flexible lawful basis for processing personal data—covering a broad range of cases (e.g., maintaining the proper functioning of websites, securing premises, or improving products or services).

However, when choosing to rely on this lawful basis, the data user must conduct a legitimate interest assessment (LIA) to ensure that the processing activity meets the following cumulative conditions:

- **Legitimacy:** The interest pursued by the data user must be legitimate;
- **Necessity:** The processing activity must be strictly necessary to achieve the pursued interest; and
- **Proportionality:** The processing activity must be proportionate, ensuring that the pursued interest does not override the data subject's rights and freedoms.

Example:

A sports club sought to generate revenues by selling member data, such as names and contact details, to external sponsors, relying on legitimate interest as their lawful basis.

Such processing activity is not lawful as the data subjects' rights and freedoms override the club's interests to generate revenues.

5. Claim or Defence of a Legal Right

For the processing activity to be considered valid, it must be strictly necessary to claim or defend a legal right.

Example:

A service provider stores client files invoking the exercise or defence of legal claims as their lawful basis. However, since the statute of limitations for initiating such claims had already run out, such retention is unlawful.

6. Execution of Court Judgments or Orders from Competent Investigative Authorities

To be considered valid, the processing activity must be strictly necessary to abide by court judgments or to execute orders given by competent investigative authorities.

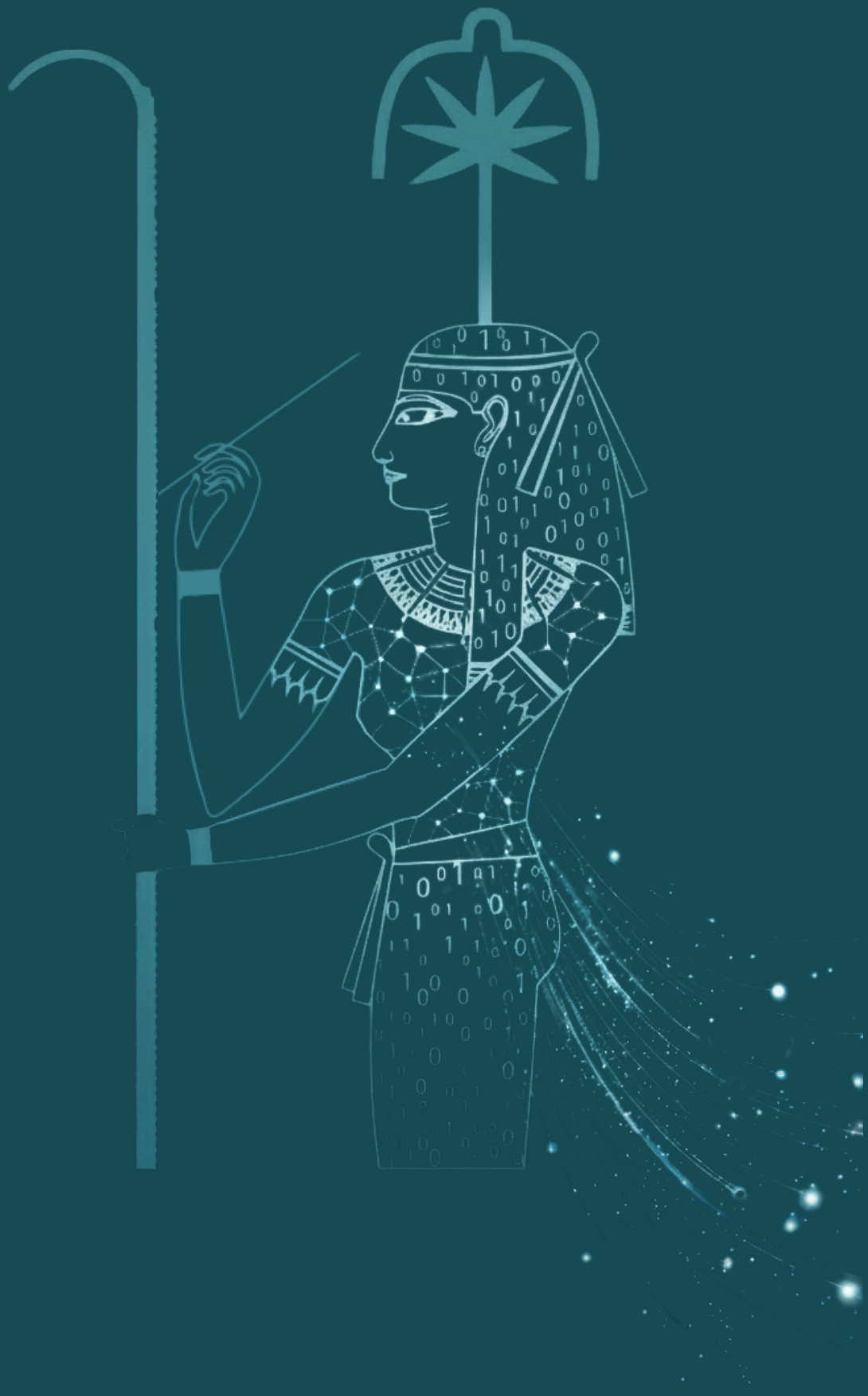
Example:

A court issues a judgment requiring a non-banking financial institution to provide financial records of an individual as part of legal proceedings. Such processing activity may be deemed lawful under the basis of execution of court judgments.

For all lawful bases requiring the necessity condition:

The necessity condition prescribed in multiple lawful bases must be strictly assessed in accordance with the data minimisation principle, requiring the data user to ensure that the processing activity is relevant, adequate, and necessary in relation to the intended purpose.

- **Relevant:** The personal data maintains a logical link and functional connection to the intended purpose.
- **Adequate:** The personal data is sufficient, in amount and nature, to effectively fulfil the intended purpose.
- **Necessary:** The personal data is strictly limited to the minimum required to achieve the purpose, with no less intrusive alternatives available.



@pdpceg

info@pdpc.gov.eg