مركز حماية البيانات الشخصية
PDPC
Personal Data Protection Center

DATA SUBJECT CONSENT 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. Appropriateness of Consent as a Lawful Basis 3
2. Conditions for Valid Consent 3
2.1. General Conditions 3
2.2. Additional Conditions for Sensitive Personal Data 4
3. Requirements of Consent Requests 4
3.1. Content of Consent Requests 4
3.2. Design of Consent Requests 4
3.3. Additional Design Requirements for Sensitive Personal Data 9
4. Management of Consent 9
4.1. Preference Management Tools 9
4.2. Refreshing Consent 9
5. The Right to Withdraw Consent 10
5.1. Ensuring Effective Withdrawal 10
5.2. Post-Withdrawal Responsibilities 11
6. Consent Records 11

Introduction

Pursuant to the Personal Data Protection Law (PDPL), all processing activities of personal data must be lawful (Article 3), meaning they must rely on at least one of the six lawful bases enumerated under Article 6, namely:

1. The 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.

Consent requires a clear and affirmative action from the data subject, showing that they agree to the use of their personal data for specific and clearly defined purposes. Given the nature of consent, relying on this lawful basis can be challenging in practice and requires strict conditions. Accordingly, data users must ensure that consent is the appropriate lawful basis for the processing activity in question, that it is obtained in a valid manner, managed responsibly throughout the entire processing lifecycle, and properly documented to demonstrate compliance when required.

This guideline sets out:

1. Appropriateness of consent as a lawful basis;
2. Conditions for valid consent;
3. Structure of consent requests;
4. Management of consent;
5. Right to withdraw consent; and
6. Consent records.

For more information on the lawful bases of processing, please refer to the Lawful Bases Guideline.

1. Appropriateness of Consent as a Lawful Basis

The validity conditions for data subject consent are stringent. Accordingly, before relying on consent, data users are advised to assess whether it is an appropriate lawful basis for the intended processing activity.

Consent is generally appropriate where data users can provide data subjects with a genuine choice to accept, refuse, or withdraw consent for the processing of their personal data. If such genuine choice and control cannot be offered, another lawful basis may be more appropriate. Notably, the selection of the lawful basis must always be determined on a case-by-case basis, taking into account the specific processing activity, the purpose, and context.

For instance, consent may not be the most appropriate in the following situations:

- **Power imbalance**: Where there is a clear power imbalance between the data user and the data subject (e.g., employment relationship), the data subject may feel pressure to consent to the processing of their personal data, making it difficult for data users to demonstrate that such consent was freely given.

- **Processing regardless of consent:** A data user must not rely on consent where the processing will occur irrespective of whether consent is refused or withdrawn, as this renders the choice afforded to data subjects illusory (e.g., requesting data subjects' consent for CCTV installed in a mall where recording occurs regardless of their choice).

Accordingly, assessing the appropriateness of the lawful basis at the outset helps to reduce the risk of future compliance issues.

2. Conditions for Valid Consent

To be deemed valid, consent must, at all times, meet a set of general validity conditions. Moreover, the processing of sensitive personal data requires the fulfilment of additional conditions.

2.1. General Conditions

To be deemed valid, consent must be:

- **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.

- **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.

2.2. Additional Conditions for Sensitive Personal Data

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

- **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, consent can be provided by either the child or the guardian, as long as the guardian is aware of the child's consent.

3. Requirements of Consent Requests

A consent request is the mechanism through which data users seek and obtain data subjects' acceptance to the processing of their personal data. To ensure compliance, consent requests must be designed in a manner that ensures that the consent obtained allows the fulfilment of the above-mentioned validity conditions.

3.1. Content of Consent Requests

Consent requests must clearly cover, at minimum, the following information:

- The identity of the data user;
- The purpose(s) of processing;
- The categories of personal data that will be processed; and
- The right to withdraw consent at any time.

3.2. Design of Consent Requests

Consent requests must be designed to meet the following requirements:

- In Arabic;
- Intelligible;

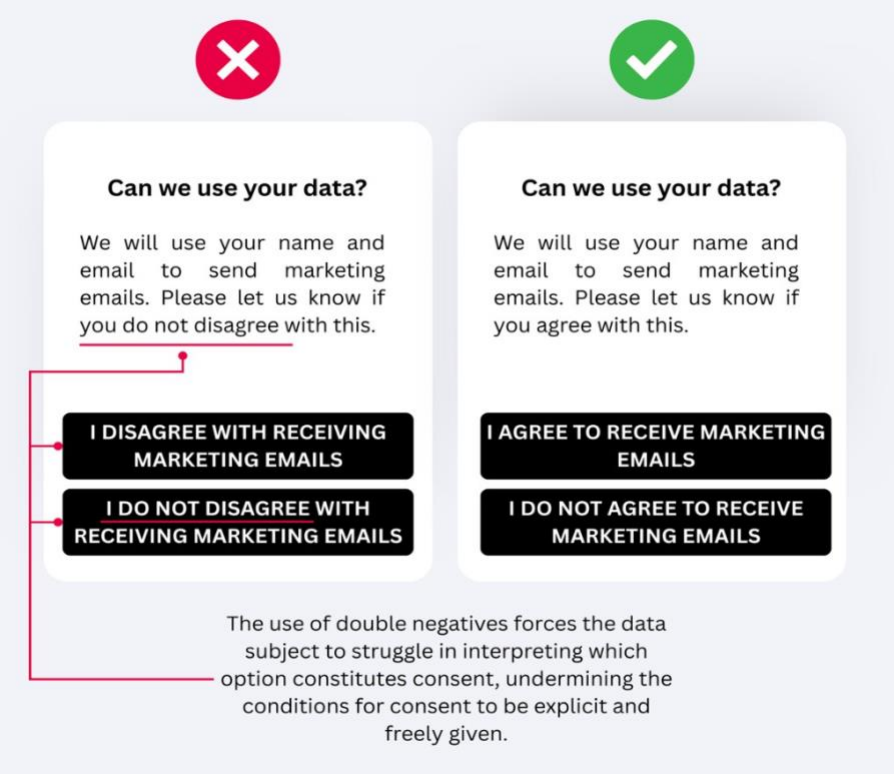
- Concise;
- Requesting affirmative action;
- Granular;
- Separate; and
- Visible and prominent.

a. In Arabic

Consent requests must be provided in Arabic as the primary language. Data users remain free to add other languages depending on their business needs.

b. Intelligible

Wording must be plain, clear, and free from complex legal or technical jargon, vagueness, ambiguity, double negatives, or inconsistencies.

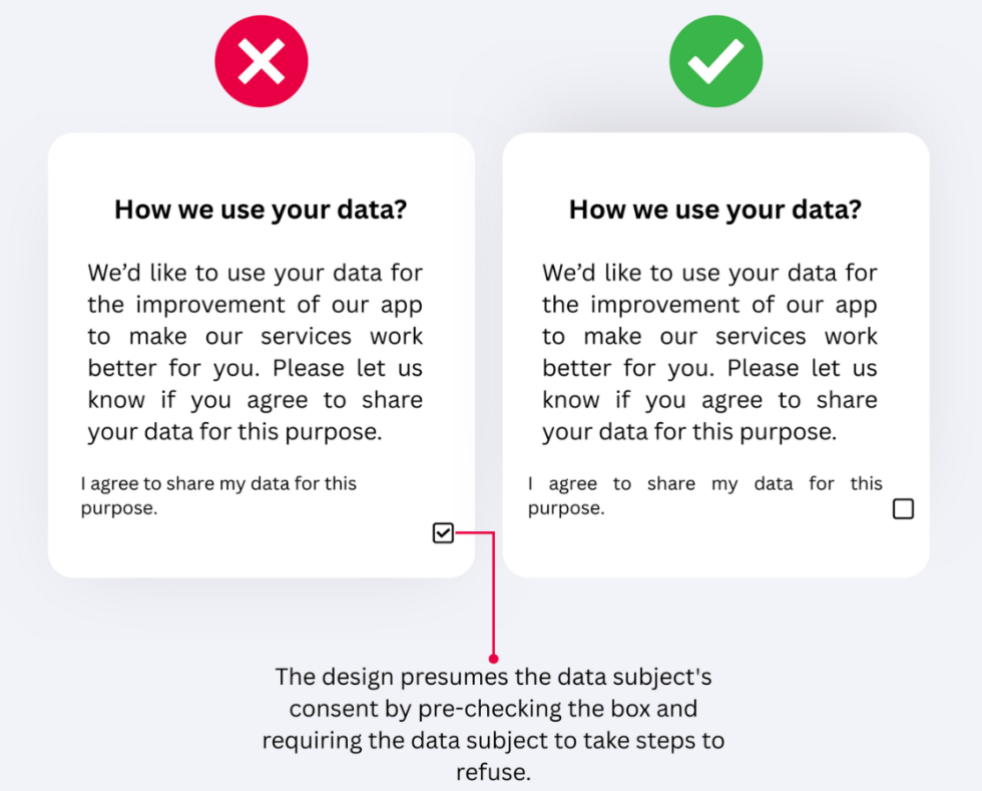


c. Concise

The information provided must be precise and straightforward, using short sentences and organised paragraphs.

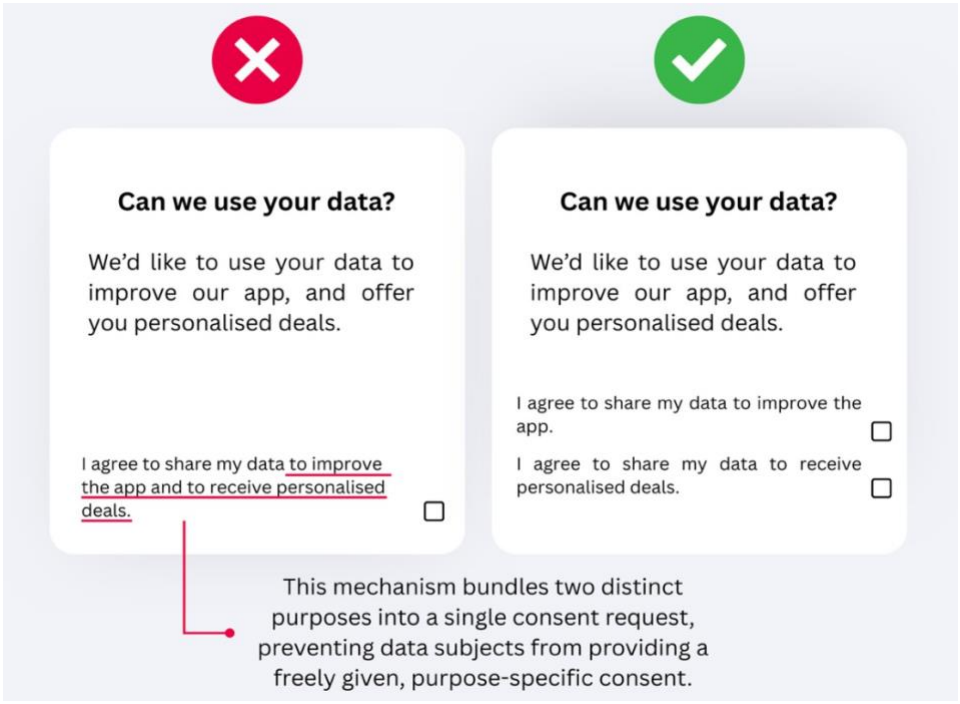
d. Requesting Affirmative Action

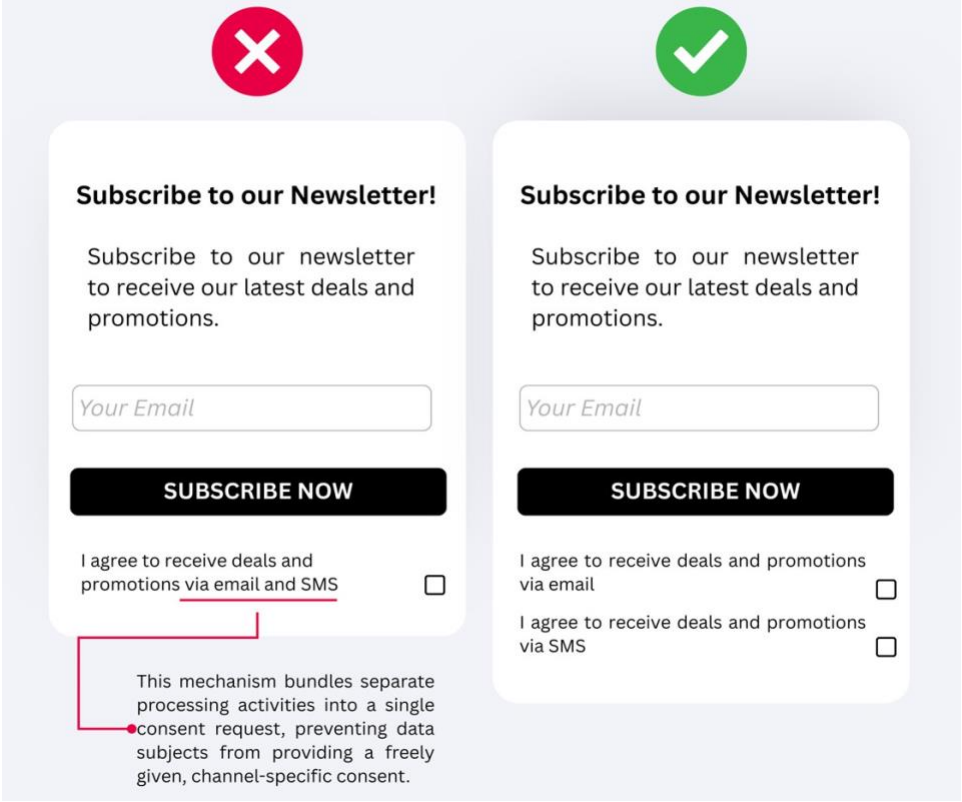
Consent requests cannot rely on implicit or presumed consent, default mechanisms such as pre-checked boxes.



e. Granular

Where relevant, separate consent should be obtained for distinct purposes or processing activities.





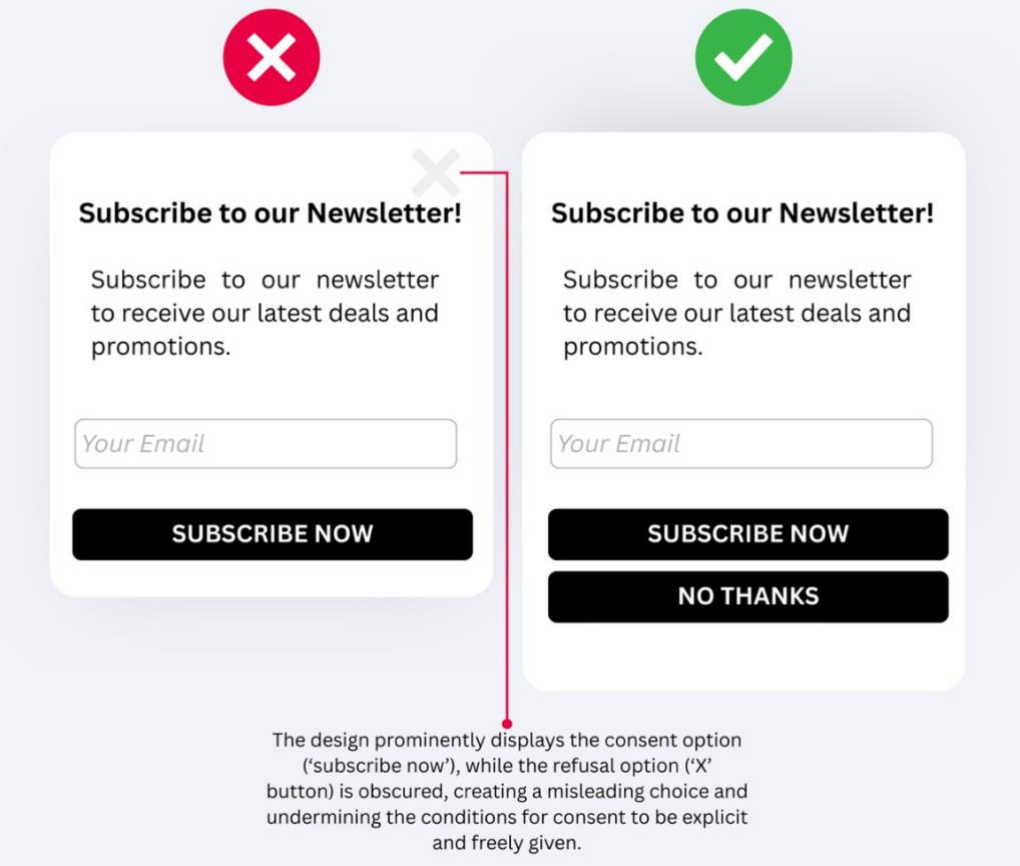
f. Separate

Consent requests must be standalone, i.e., kept separate from general terms and conditions, privacy notices, etc.

> **Note:**
>
> Consent requests and privacy notices serve two different purposes. The privacy notice ensures that the data subject is informed about the processing of their personal data regardless of the lawful basis relied upon, whereas the consent requests focus on obtaining the data subject's valid consent.

g. Visible and Prominent

Data subjects must be offered a clear and prominent choice to accept or refuse consent. Data users must avoid the use of dark patterns, which are deceptive design features that manipulate users into consenting (e.g., hiding or obscuring the "refuse" option, or visually emphasising the "accept" option).



> **Example:**
>
> A school introduces facial-recognition technology for cashless canteen payments. In terms of consent, they relied on an opt-out slip sent to parents. Parents were deemed to have consented unless they returned the slip to refuse participation. This method of obtaining consent is invalid as data users cannot rely on presumed consent to process data subjects' personal data.

3.3. Additional Design Requirements for Sensitive Personal Data

Data users relying on consent to process sensitive data, including children's data, must ensure that the consent requests meet the following additional conditions:

- **Written Consent:** Implementing mechanisms to record and retain written consent when processing sensitive data; and
- **Age Verification Measures:** Establishing proportionate verification processes to determine whether the data subject meets the required age threshold or whether guardian consent is necessary.

4. Management of Consent

Once consent has been obtained, data users must ensure that it is properly managed by providing data subjects with preference-management tools and ensuring consent is refreshed.

4.1. Preference Management Tools

Data subjects must be provided with ongoing choice and control over their consent. This may be ensured through accessible and user-friendly preference management tools (e.g., privacy dashboards), which enable data subjects to access, manage, and update their consent settings at any time.

4.2. Refreshing Consent

Data users must ensure that consent remains valid and up-to-date, and reflects the processing activity. Accordingly, data users are advised to refresh consent at appropriate intervals, particularly where relying on the original consent may no longer be sufficient. This is especially necessary when parental consent was obtained for a child who has since reached the age of consent, in which case the data user must obtain the individual's own consent.

Consent must also be refreshed whenever the processing activity or the purposes substantially change, as the original consent will no longer constitute a valid lawful basis. In such cases, the data user must obtain new consent that accurately reflects the updated processing activity or purpose.

5. The Right to Withdraw Consent

Data users must ensure that data subjects can effectively exercise their right to withdraw consent throughout the processing activity lifecycle.

5.1. Ensuring Effective Withdrawal

For consent to remain freely given, it must also be freely revocable, meaning data users must:

a) Inform data subjects, prior to or at the time of obtaining consent, of their right to withdraw consent at any time and the manner in which it may be exercised;

b) Provide a withdrawal mechanism that is clear, simple, accessible, user-friendly, and free from any hidden settings or unnecessary requirements, and ideally through the same method by which consent was given;

> **Example:**
>
> A marketing agency implements a withdrawal mechanism requiring data subjects to first click an "unsubscribe" link in emails and then send a separate email explaining the reasons for withdrawal.
>
> This withdrawal mechanism is not valid, as it creates unnecessary obstacles for data subjects and prevents them from easily withdrawing their consent.

c) Ensure withdrawal of consent is free of charge;

d) Enable withdrawal of consent at any time; and

e) Ensure that withdrawal of consent is without adverse consequences to data subjects, meaning it does not result in any penalty, limitation, or loss of services to the withdrawn consent.

> **Example:**
>
> An email service provider designs their platform so that data subjects must consent to marketing cookies to continue using their email services. If they attempt to withdraw consent, data subjects are warned that such withdrawal will result in the loss of access to their email accounts. No alternative options are provided, thereby compelling users to either accept these non-essential cookies or abandon the service entirely.
>
> This practice is unlawful as the right to withdraw consent must be free and cannot be tied to abandoning irrelevant services.

5.2. Post-Withdrawal Responsibilities

Upon data subjects' withdrawal of consent, data users shall:

- Cease all processing activities based on the withdrawn consent without undue delay;
- Synchronise withdrawal across all relevant systems, if applicable;
- Notify any data recipients of the consent withdrawal, if applicable; and
- Record the withdrawal, including its time and date.

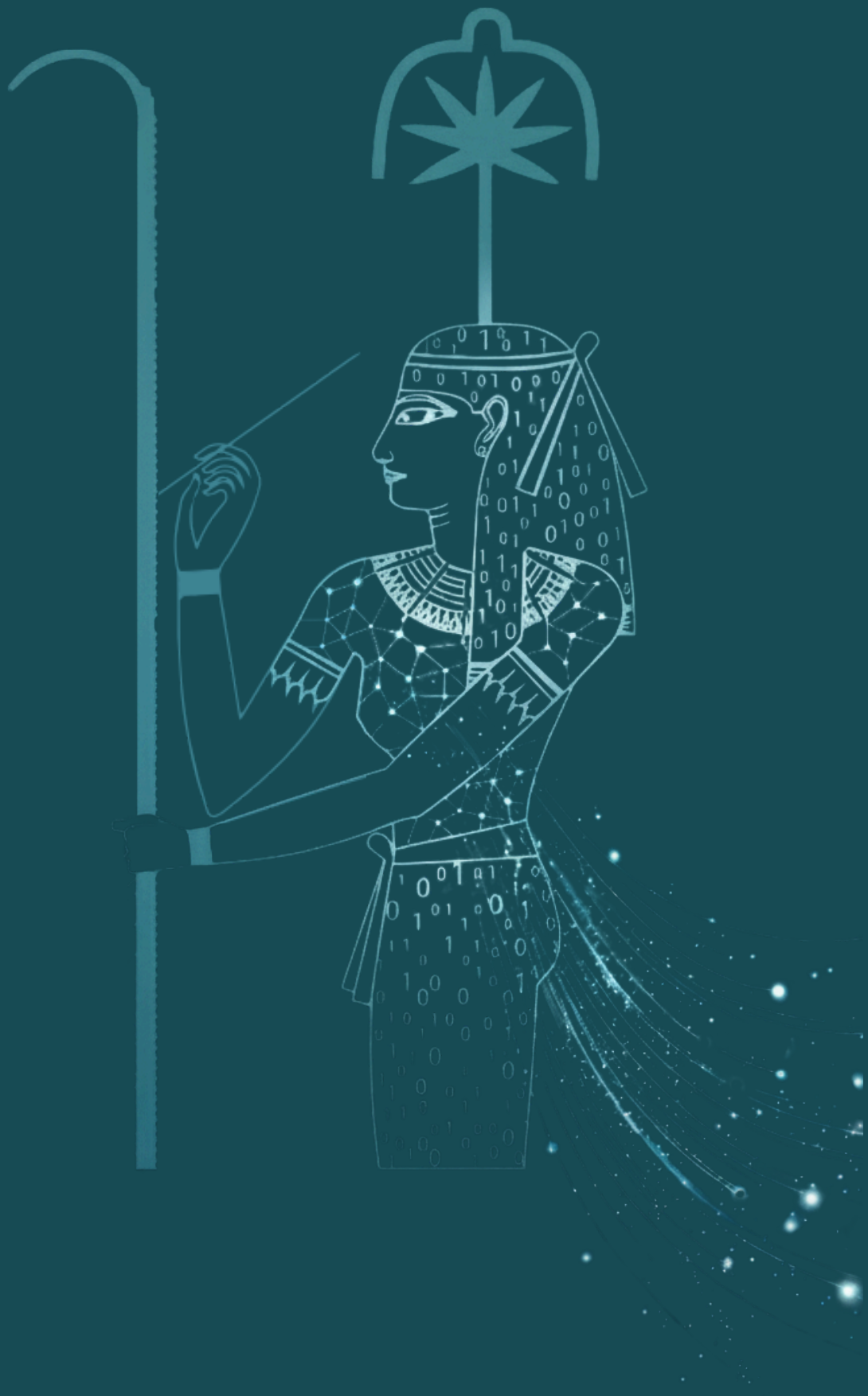
> **Note:**
>
> Withdrawal of consent does not affect the lawfulness of processing activities carried out prior to the withdrawal, provided that the initial consent was valid.

6. Consent Records

Maintaining records of consent is a key element of accountability. It enables data users to demonstrate at any time that valid consent was obtained under the proper conditions. Such records must be accurate, regularly updated, and made available to the PDPC upon request.

Consent records must contain, at minimum, the following information:

- **Who consented:** the data subject's name or unique identifier;
- **When consent was obtained:** the date and time (e.g., digital timestamp);
- **Information provided:** details of the information provided to the data subject in the consent request;
- **How consent was given:** the affirmative action taken by the data subject to authorise the processing; and
- **Withdrawal of consent:** whether the data subject has exercised their right to withdraw consent, and if so, the date and time of withdrawal.



@pdpceg

info@pdpc.gov.eg