مركز حماية
البيانات الشخصية
PDPC
Personal Data Protection Center

DATA PROTECTION PRINCIPLES 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 Personal Data Protection Law (PDPL) sets out fundamental principles governing the processing of personal data. Adhering to these principles is essential for compliance with data protection obligations, safeguarding the rights and freedoms of data subjects, and mitigating legal, financial, and reputational risks. These principles are:

1. Lawfulness;
2. Fairness;
3. Transparency;
4. Purpose limitation;
5. Data minimisation;
6. Data accuracy;
7. Storage limitation;
8. Data security; and
9. Accountability.

1. Lawfulness

To lawfully process personal data, data users must rely on at least one of the following lawful bases enumerated under Article 6 of the PDPL:

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

The lawful basis must be identified before initiating the processing activity, properly documented, and, where applicable, communicated to the data subject.

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

2. Fairness

Personal data shall be processed in a manner that aligns with data subjects' reasonable expectations and ensures that data subjects do not suffer any unjustifiable harm.

Therefore, before initiating a processing activity, and throughout the entire lifecycle of personal data, data users must assess whether the processing is fair, proportionate, and respectful of the data subjects' rights and freedoms.

The following factors may be considered when assessing the fairness of a processing activity:

- **The transparency of the information provided to the data subject:** whether the data subject is effectively provided with sufficient information in a clear and plain language (e.g., using vague or generic statements such as "we may use your data for various purposes" without identifying the actual purposes or categories of processing is not considered as transparent information).

  For more information on transparency, please refer to section 3.

  For more information on privacy notices, please refer to the Privacy Notice Guideline.

- **The reasonable expectations of data subjects:** whether the data subject could reasonably anticipate the processing activities (e.g., a data subject would not reasonably expect the presence of CCTV inside fitting rooms).

- **The risks to data subjects' rights and freedoms:** whether the processing may result in harm to the data subject, such as discrimination, bias, or any other significant impacts (e.g., an online retailer charging different prices to users for the same product based on inferred personal data).

- **The collection source of personal data:** whether the data was collected directly from the data subject or obtained indirectly via a third party (e.g., a data subject would not reasonably expect to receive marketing communications from a controller with whom they have had no prior interaction or relationship).
- **The vulnerability of the data subject:** whether the processing involves individuals who may have a reduced ability to understand the processing or exercise their rights, such as minors, the elderly, or individuals with disabilities (e.g., a doctor specialising in elderly care provides their privacy notice only through electronic means).
- **The use of automated decision-making and profiling:** whether the processing involves automated decisions producing legal or significant effects on the data subject without human oversight (e.g., an HR system automatically rejecting candidates based on ethnicity).

> **Example:**
>
> A car manufacturing company launches a new smart service offering drivers features such as intelligent navigation, roadside assistance, and insights into driving behaviour.
>
> To provide these features, the company collected detailed driving data—including speed, acceleration, and hard braking patterns, and stated in their privacy notice that the purpose of processing was to enhance driving safety.
>
> However, the company sold this data to insurance providers without informing drivers, which led to increased insurance premiums for some data subjects.
>
> This practice violates the fairness principle, as personal data was processed in ways that data subjects could not reasonably expect and that resulted in harm to their rights and freedoms.

3. Transparency

Personal data must be processed in a manner that is transparent, clear, and honest towards the data subject.

The information provided to the data subjects must be:

- **Concise:** The information must be precise and straightforward, using short sentences and organised paragraphs.
- **Transparent:** The information must be honest, not misleading or incomplete.
- **Easily accessible:** The information must be made easily available to data subjects without undue effort to locate.

- **Intelligible:** The information must be provided using plain and understandable language, taking into consideration the characteristics of targeted data subjects.
- **Provided in a timely manner:** The information must be provided without undue delay and within the required timeframes.
- **Accurate and up to date:** The information must be accurate and regularly updated.

The transparency principle may arise, inter alia, in the following circumstances:

- At the time of data collection.
- Upon the data subject's request.
- In case of a data breach.

> **Example:**
>
> An online platform designs their privacy notice using confusing legal language, with key information scattered across multiple pages. As a result, data subjects struggled to understand how their personal data was handled.
>
> This practice violates the transparency principle, as information was not presented in a concise, transparent, and intelligible manner.

4. Purpose Limitation

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

Personal data must be collected and processed for specified, explicit, and legitimate purposes:

- **Specified:** The purpose must be clearly identified prior to the processing activity, without being vague or ambiguous.
- **Explicit:** The purpose must be clearly communicated to data subjects in a transparent manner, ensuring they are enabled to fully understand why their personal data will be processed.
- **Legitimate:** The purpose must not violate any applicable laws and regulations.

Furthermore, once personal data has been collected, any further processing must be limited to the originally intended purpose(s), unless another lawful basis explicitly permitting further processing supports the new processing activity.

Example 1:

An E-commerce company informs customers that the purpose of the processing activity is “business purposes”. This practice violates the purpose limitation principle, as such purpose is vague and lacks specificity, preventing customers from understanding the exact reasons for data collection. Instead, the company could have clearly defined and communicated specific purposes such as "delivering orders” or “personalising marketing offers”.

Example 2:

A hospital collects and processes a patient’s personal data for the purpose of providing medical care and treatment. The hospital later wishes to use this data for marketing purposes. However, this new purpose is not compatible with the original purpose of providing medical care, and therefore, such processing cannot take place unless a new valid lawful basis is established (e.g., the patient’s explicit consent).

5. Data Minimisation

Personal data must be collected and processed only to the extent that is relevant, adequate, and necessary in relation to the intended purpose(s):

- **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 alternative available.

Example:

A railway company collects gender data from all passengers for the purpose of preventing mixing between male and female passengers in shared night-train cabins.

This generalised collection practice violates the data minimisation principle, as gender data is irrelevant for passengers who do not book shared night-train cabins.

6. Data Accuracy

All reasonable steps must be taken to ensure that the personal data is accurate, complete, and kept up-to-date, in line with the purpose(s) of the processing activity.

Any personal data that is considered inaccurate, incomplete, or outdated must be erased or rectified without undue delay, particularly where the inaccuracy of personal data could negatively impact data subjects' rights and freedoms.

To uphold data accuracy, appropriate measures may include:

- Assessing the reliability of the data source prior to collection;
- Verifying the accuracy of the data through monitoring systems, periodic reviews, and validation mechanisms;
- Exercising due diligence when integrating and consolidating data from multiple sources or datasets;
- Implementing effective identity management controls to ensure consistency of data across systems; and
- Enabling the data subject's right to rectification.

> **Example:**
>
> A healthcare provider operating several branches registered patients separately at each facility without a unified master patient index or central identity management system.
>
> As a result, the same patient was recorded under different identifiers across branches, with each profile containing partial medical information, leading to inconsistent records and missing clinical data during treatment.
>
> This practice violates the data accuracy principle, as it results in incomplete and unreliable patient records, creating high risks for data subjects.

It should be noted that, under the PDPL, records containing past inaccuracies may be considered "accurate", having regard to the purpose of the processing activity, provided that such data is not misleading and that the retention of such personal data is necessary for justifiable reasons.

> **Example:**
>
> A doctor retains their patient's past misdiagnosis in their medical records for the purposes of understanding the necessary course of treatment and understanding any additional health problems that may arise in the future.

7. Storage Limitation

Personal data must not be retained for longer than necessary to achieve the purpose(s) of the processing activity. Once the identification of data subjects is no longer required, the personal data must be either securely erased or appropriately anonymised.

To ensure compliance, before initiating the processing activity, personal data retention periods, or at least the criteria for determining them, must be clearly defined, documented, and, where necessary, set out in a data retention policy to uphold accountability.

When determining data retention periods, the following factors may be considered:

- The duration for which the personal data remains necessary to achieve the specific purpose(s) for which personal data is processed.
- Any applicable legal, regulatory, or contractual obligations that require data to be retained for a specified period (e.g., storing clients' personal data for five years following account closure, in accordance with Article 9 of the Anti-Money Laundering Law, as enacted by Law No. 80 of the year 2002).
- The necessity of retaining certain categories of personal data for the establishment, exercise, or defence of legal claims, provided that the retention of such data is relevant, adequate, and necessary.
- Situations where retaining personal data is required to demonstrate the existence of a prior relationship with the data subject.
- The duration for which recipients are required to retain the shared personal data.

> **Example:**
>
> A company permanently stores customer service call recordings to evaluate employee performance and improve customer interactions.
>
> This practice violates the storage limitation principle, as retaining the recordings for a short, defined period would have been sufficient to achieve the stated purpose.

8. Data Security

Personal data must be secured throughout its entire lifecycle against unlawful or unauthorised processing, access, alteration, damage, loss, or destruction.

To this end, appropriate technical and organisational measures must be implemented to ensure the integrity, confidentiality, availability of both the personal data and the processing systems, as well as to maintain the resilience of those systems. Moreover, where processing activities present a high risk to the rights and freedoms of data subjects, proportionate and, where necessary, enhanced security measures must be implemented.

9. Accountability

Appropriate technical and organisational measures must be implemented to ensure that personal data is processed in compliance with all data protection principles and obligations. Furthermore, compliance must be demonstrable through appropriate documentation, in accordance with the data protection regulatory framework.

Key accountability measures may include, inter alia:

- Obtaining the necessary licences and permits.
- Maintaining records of processing activities (RoPA).
- Maintaining a record of security incidents.
- Maintaining a record of data subjects' requests.
- Conducting data protection impact assessments (DPIA) when needed, and maintaining the underlying documentation.
- Conducting legitimate interest assessments (LIA) when needed, and maintaining the underlying documentation.
- Conducting transfer impact assessment (TIA) when needed, and maintaining the underlying documentation.
- Providing regular employee training and awareness initiatives on different data protection obligations, and maintaining records of their completion.
- Implementing appropriate internal privacy policies.
- Performing regular privacy audits, and maintaining reports of such audits.
- Incorporating appropriate data protection clauses in data processing and sharing agreements.