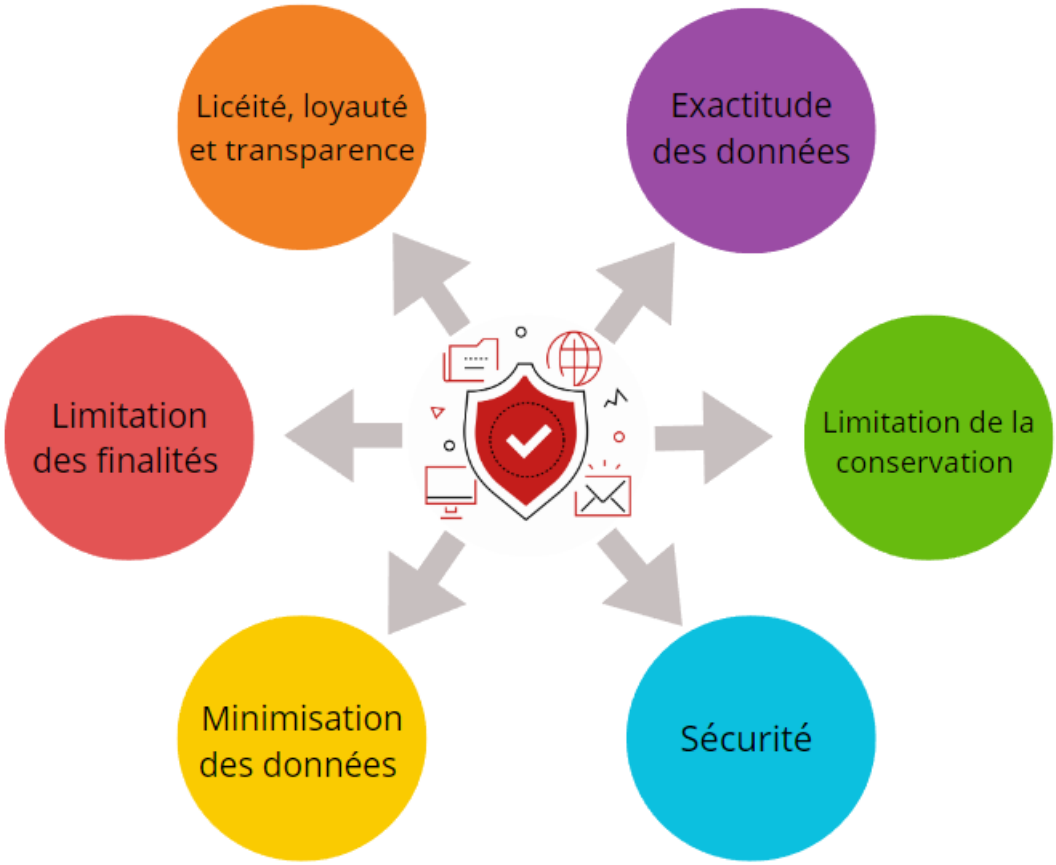
The main principles of personal data protection

Article 4 of Law no. 1.565 of December 3, 2024 lists the 6 main principles of personal data protection that all data controllers must respect.

These are as follows:

- the lawfulness, fairness, and transparency principle;
- the purpose limitation principle;
- the data minimization principle;
- the data accuracy principle;
- the storage limitation principle; and
- the data security principle.



The lawfulness, fairness, and transparency principle

Lawfulness

In accordance with Article 5 of Law no. 1.565 of December 3, 2024, in order to be lawful, personal data processing must meet at least one of the following 6 requirements:

- obtaining the **consent** of the data subject for **one or more specific purposes**;

What is meant by the data subject's consent ?
Consent is defined in Article 2 of the Law as « *any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her* ». Data subjects must therefore give their consent to the processing of their personal data in a **free, specific, informed and unambiguous manner, by means of a clear positive** act. [For more information, refer to the factsheet **The consent of data subjects**]

Example: a website provides two boxes to tick when it collects the email address of Internet users, the first one to authorize the sending of the newsletter, the second one to consent to the sending of commercial offers.

- the requirement to comply with a **legal obligation** to which the data controller is subject;

  Example: processing relating to anti-money laundering obligations implemented by banks

- the necessity for the performance of **a contract** to which the data subject is a party or of **for the performance of pre-contractual measures taken** at the request of the data subject;

  Example: the collection of the name and postal address of the recipient is necessary for the delivery of an order placed online

- necessary to **protect the vital interests** of the data subject or those of another natural person;

  Example: the processing implemented by a doctor for the medical follow-up of his or her patients;

- the existence of **public interest reasons** when the processing is carried out by a legal person governed by public law or by a legal person governed by private law entrusted with a mission of general interest or a public service concession;

  Example: the processing by an administrative department of data related to the monitoring of people placed in shelters

- necessary for the purposes of a **legitimate interest** pursued by the data controller or by a third party, **except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject** which require protection, in particular where the data subject is **a minor**.

What questions should be asked when assessing legitimate interest ?
1st step : identify a legitimate interest : why do you want to process the data? What are you trying to achieve ? Who benefits from the processing ? What would be the impact if you could not go ahead? Would the use of the data be unethical or unlawful in any way? Etc. **2nd step : demonstrate that the processing is necessary to achieve it :** does the processing actually help to further the interest? Is it a reasonable way to go about it? Is there another less intrusive way to achieve the same result? Etc.... **3rd step : strike a balance between this legitimate interest and the interests, rights and freedoms of the data subjects** : are certain data considered sensitive? Would the user reasonably expect the data to be used in this way? Could some users object and say that it is too intrusive? What impact will the data processing have on the data subjects? What safeguards can be put in place to minimize the impact? Etc.

Example *:* a jewellery store wants to install a video surveillance system for security purposes. Its legitimate interest is the protection of its premises and the valuable goods they contain. The system will act as a deterrent, as a sign at the entrance will indicate that the premises are under video surveillance, and the images collected by the cameras will allow evidence to be gathered in the event of any offences. Lastly, the rights of the data subjects will be protected, as they will be informed by the sign at the entrance and the cameras will only be installed in the most sensitive areas, i.e. the entrance and sales areas.

Processing carried out by a legal person governed by public law or by a legal person governed by private law entrusted with a mission of general interest or a public service concession in the performance of their tasks may not be based on legitimate interest. In this case, these bodies may use the **public interest** ground to justify their processing.

However, these bodies may base their processing on legitimate interest, provided that they do not fall within their public service missions. Examples include the processing of data relating to their own staff or employees, purely internal activities, or services that **are not offered as part of their public service missions**

When data are processed for a **purpose other than that for which they were originally collected**, the data controller must **ensure that further processing is compatible with the purpose for which the data were originally collected**. To this end, he/she may take into account :

- the **possible relationship** between the initial purposes and the purposes of the planned subsequent processing;
- the **context** in which the personal data have been collected, in particular with regard to the relationship between the data subjects and the data controller;
- the **nature of the personal data**, in particular if the processing involves sensitive data or data relating to offences and criminal convictions;
- the **possible consequences of the planned further processing** for the data subjects;
- the **existence of appropriate safeguards**, which may include encryption or pseudonymisation.

What does encryption mean ?

The term « *encryption* » refers to a **reversible** process that makes the information in a document **unreadable** in order to preserve its **confidentiality**.

After encryption, it is always possible to retrieve the data originally encrypted using a key, i.e. a decryption algorithm.

What is pseudonymisation ?
Pseudonymisation is a process that consists of **replacing directly identifying data** (surname, first name, etc.) **with indirectly identifying data** (personnel number, social security number, number plate, telephone number, etc.). However, pseudonymisation should not be confused with **anonymisation**, which is a process that **irreversibly** neutralises data. Anonymised data can no longer be used to directly or indirectly identify an individual. Pseudonymised data **remains in legal terms personal data**, unlike anonymised data.

Fairness

Personal data must also be **processed fairly**. This means that the data subject must be informed of the risk of impact on his or her privacy in order to ensure that the processing does not have any unforeseeable negative effects.

Transparency

Finally, personal data must be processed **in a transparent manner**. The principle of transparency means that the data controller must provide the data subject with a certain amount of information about the processing operations (purpose(s), identity of the data controller and contact details, storage period, recipients, etc.) and their compliance at the time of treatment.

[For more information, refer to the factsheet **Information to be provided to the data subjects]**

The purpose limitation principle

Personal data may be collected for **several purposes**, providing that these purposes are:

- **specific** ;
- **explicit** ;
- **legitimate**.

Furthermore, the data must not be further processed in a way incompatible with these purposes.

Example of a compliant purpose: a company's marketing department may collect its customers' email addresses for the purpose of sending promotional offers

Example of a non-compliant purpose: a telephone operator collects the data subject's email address for the purpose of sending monthly invoices **and** for any other processing the operator chooses.

However, further processing for archival purposes in the public interest, for scientific or historical research, or for statistical purposes, is considered compatible with the initial purposes of collection, provided that **appropriate safeguards have been put in place**.

This exception does not apply to processing:

- implemented for the purposes of prevention, detection, investigation, and prosecution of criminal offenses or the execution of criminal sanctions, including protection against and prevention of threats to public security;

- that are relevant to national security.

The data minimization principle

A data controller should ensure that the data collected are "*limited*" to the purpose of the processing.

To comply with this principle, the collected personal data must be:

- **adequate**,
- **relevant**; and
- **limited** to what is necessary in relation to the purposes of the processing.

Example: an online store that wishes to send a promotional offer for its customers' birthdays doesn't need to know their year of birth. Only the day and month are required.

The data accuracy principle

The personal data processed must be **accurate** and, where necessary, **kept up to date**.

The data controller shall take **reasonable measures**, that is, measures that do not require **disproportionate** effort, to ensure that inaccurate or incomplete data are erased or rectified **as soon as possible**.

The principle of data accuracy must be respected for **each** processing implemented by the data controller and must be assessed **in the context** of the purpose of the data processing.

In some cases, it may not be possible to update the data. These are cases where the purpose is essentially to document events as a historical "*snapshot*". For example, a medical report cannot be updated, even if it is later found that the conclusions it contains were inaccurate. Only additions may be made, provided they are clearly identified as contributions made at a later date.

Conversely, in certain situations, it is **absolutely necessary** to keep data up to date and accurate because of the potential harm that could be caused to the data subject if the data are inaccurate.

Example: special databases that contain personal credit history data. These databases are very useful for banking institutions as they enable them to check the creditworthiness of potential customer in order to obtain a loan.

The storage limitation principle

The personal data collected **cannot be kept indefinitely** in a form which permits identification of the data subjects. As a result, practice has made it possible to identify 3 phases in the storage of data: storage in the active database and intermediate data archiving, which together make up the **administrative useful life**, and definite data archiving.

Storage in the active database

Personal data are kept in the active database for **as long as is necessary for the purposes** for which they were collected.

They are kept in such a way that they are **easily accessible** to those **responsible for processing the request**.

Examples :

- personal data supplied via a contact form for the time required to process the request
- a job application

Intermediate data archiving

Once the purpose has been fulfilled, certain data must be stored in an intermediate database.

These are data:

- of **administrative interest to the organization**

Example : retention of data/documents in the event of litigation

Or

- that are subject to a **legal obligation**.

Example: retention of billing data

Definite data archiving

Certain data may be kept for a longer period if they are processed exclusively for archival purposes in the public interest, for scientific or historical research or for statistical purposes, subject to the **existence of appropriate safeguards**.

The data security principle

The processing operations put in place must guarantee **appropriate security of personal data** in order to prevent any adverse effects for the data subject, including protection against unauthorized or unlawful processing or against accidental loss, destruction or damage.

To this end, the controller must take the necessary **technical and/or organizational measures** to guarantee the integrity and confidentiality of the data.

The appropriateness of the measures must be **determined on a case-by-case basis and reviewed regularly.**