

Information to be provided to the data subjects

Article 10 of Law no. 1.565 of December 3, 2024 imposes the obligation on the data controller to take **appropriate measures** to provide the data subject with any information on the use of his or her data and to facilitate the exercise of his or her rights. This is what is known as the principle of **transparency**.

Under this principle, all data subjects **must** receive information on how their data are used (who collects their data? for what purpose(s)? for how long? what rights do they have? etc.) so that they can keep control of them.

With this information, the data subject will then be in a position, if need be, to **assert his or her rights** and hold the data controllers accountable for the processing of his or her personal data.

This transparency obligation applies **throughout the processing life cycle**.



This right does not apply to processing operations relating to national security.



What information should be provided?

This principle of transparency implies a **proactive attitude** on the part of the data controller.

Article 11 of Law no. 1.565 of December 3, 2024 sets out the information that must be provided by the data controller to the data subjects.

This information may differ depending on **whether or not** the data have been collected **directly** from the data subjects.



Where the data subject already has this information, the data controller shall not be obliged to provide him/her with the information referred to in Article 11, **whether or not** the data have been obtained **directly** from the data subject.

Information to be provided when data are collected directly from the data subject

When are data collected directly from the data subject?

According to the Article 29 Working Party¹ guidelines on transparency, adopted on November 29, 2017 (revised and adopted on April 11, 2018), **direct data collection** occurs in two cases:

- when the data **consciously** provides the data to a data controller.

Example : the person completes an online form

- when the data controller collects the person's data **by observation**.

Example : the data controller uses data capturing devices such as cameras, network equipment or Wi-Fi tracking systems.

This information, provided for in the aforementioned Article 11, is as follows:

1. **The identity and contact details of the data controller**, and where applicable, its **representative** established in Monaco or, failing that, within a Member State of the European Union.

This information must make it **easy to identify** the data controller and facilitate all forms of communication with him/her.

Examples: telephone number, email address or postal address

2. The **purposes** and **legal basis** for the processing.

A purpose is the **main objective** pursued by the data controller. In order to be lawful, data processing must meet at least one of the 6 requirements set out in Article 5 of Law no. 1.565 of December 3, 2024, namely:

- the consent of the data subject
- compliance with a legal obligation
- performance of a contract
- safeguarding the vital interests of the data subject
- a reason of public interest
- to fulfil a legitimate interest

Example : setting up a video surveillance system in a shop based on the **legitimate interest pursued by the data controller**, i.e. the protection of assets and individuals

¹ Independent European Union advisory board which dealt with issues relating to the protection of privacy and personal data until May 25, 2018 (before the entry into force of the General Data Protection Regulation - GDPR).



Where processing is based on the **legitimate interests** pursued by the controller, those interests must not adversely affect the **interests or fundamental rights and freedoms of the data subjects**.

Consequently, in the interests of good practice, the controller may provide the data subject with the information resulting from the balancing of this legitimate interest against the interests or fundamental rights and freedoms of the data subject.

Example: in the case of video surveillance, it may be specified that the objective is solely security-related (legitimate interest of the data controller) and will not lead to the monitoring of employees' work and/or working hours (interests of the data subjects)

3. The **legitimate interests pursued by the data controller** or a third party where legitimate interests is the legal basis.
4. The **categories of personal data** concerned.

The data controller does not have to give details of all the data collected and name them all, but can simply list the categories of data.

Examples :

- « *addresses et contact details* » which may include telephone numbers, postal addresses or email addresses
- « *electronic identification data* » which may include identifiers and passwords

5. The **period for which the data will be stored** or, where that is not possible, the criteria used to determine that period.

Example : length of contractual relationship + 5 years

This information is directly linked to the principles **of data minimization** and **storage limitation**.

The data controller must ensure that the data collected are not kept indefinitely, but are « *limited* » to achieving their objectives.

The retention period must be formulated in such a way that the data subject can assess, **depending on the situation in which he/she finds himself/herself**, what the retention period will be. The data controller cannot therefore simply state in general terms that personal data will be kept for as long as the purpose of the processing so requires.

If necessary, **different retention periods may be mentioned** for the **different categories** of data and/or the **different purposes** of processing, in particular for retention periods for archival purposes.

6. Whether **replies are obligatory or voluntary**, and the consequences for the data subject of failing to reply.

The obligation to provide information may result from a **legal or contractual requirement**. It may also be a **condition for concluding a contract**.

Example: the obligation to provide information to one's employer as part of the employment relationship may be a contractual obligation.



Online forms should clearly indicate which fields are « *mandatory* » and which ones are « *optional* ».

They should also state what the consequences are if the data subject fails to complete the « *mandatory* » fields.

7. The **consequences of failing to respond**.

8. Where processing is based on **consent**, the right to withdraw consent **at any time**.

This mention should also explain to the data subject how to withdraw his or her consent. In this respect, it must be **as easy** for a data subject to withdraw consent as it is to give it.

9. The **recipients** or **categories** of recipients

In accordance with Article 2 of Law no. 1.565 of 3 December 2024, a recipient is the « *natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry shall not be regarded as recipients* ».

If the data controller decides to communicate only the **categories of recipients**, the information provided should be **as specific as possible**, indicating the **type** of recipient and their **sector of activity**.

10. The means of exercising **rights of access, opposition, rectification, deletion, limitation or portability**.

This information must summarize what **these rights** include and **how they can be exercised**.

In particular, the **right to object** must be brought to the attention of the data subject **at the latest at the time of the first communication** with that person and must be presented **clearly and separately from any other information**.

11. The right to **object to the use** of their data **on behalf of third parties** or to the **communication** to third parties of personal data concerning them **for prospecting purposes**, in particular for commercial purposes.

12. The right to **lodge a complaint with the Autorité de Protection des Données Personnelles (APDP)**.

13. Where applicable, the **contact details of the Data Protection Officer**.

It is not necessary to give his/her name.

14. Where applicable, the existence of **automated decision-making**, including **profiling**, and the reasoning behind the processing.

What about automated decision-making and profiling?

An automated decision is a decision taken in respect of an individual, **by means of algorithms applied to their personal data**, without any human being intervening in the process.

Profiling is any form of processing that uses an individual's personal data to **analyze and predict their behaviour**, such as their performance at work or their lifestyle habits.

This information may include the **logic involved**, as well as the **significance and the envisaged consequences** for the data subjects.

15. Where applicable, the fact that the data controller carries out or intends to carry out a **transfer to a country, territory or international organization located outside the Principality**.

This information should mention the details of the transfers and the **relevant guarantees** (adequacy decision, standard contractual clauses, etc.).



If personal data are **subsequently processed** for a **purpose other** than that for which they were collected, the data controller must inform the data subject of this other purpose and of **any other relevant information**.

Information to be provided when data are not collected directly from the data subject

When are data not collected directly from the data subject?

For the Article 29 Working Party, this means personal data that a controller has obtained from sources such as:

- third party data controllers ;
- publically available sources ;
- data brokers ; or
- other data subjects.

Examples : commercial partners

In addition to the above information, Article 11 of Law no. 1.565 of December 3, 2024 stipulates that the following information must also be brought to the attention of the data subject when the personal data have not been collected directly from him or her:

16. The **source** from which the personal data **originate**.

The **source** must be named if it is **identifiable**. Where this is not the case, the data controller must indicate the **nature** of the source (public or private) and the **types** of organizations, companies and sectors.

Example: manufacturers of games consoles where games publishers are the recipients

However, Article 11 of Law no. 1.565 provides for **4 situations** in which the controller does not have to inform the data subject in the event of **indirect collection**:

1st situation : the provision of such information proves **impossible** or requires **disproportionate effort**;

Example : the data subject is not directly identifiable or there is no way of contacting him or her

Article 4 of Sovereign Order n° 11.327 of July 10, 2025 implementing Law No. 1.565 of December 3, 2024 on the protection of personal data provides for **two cases in particular** where the provision of information may prove impossible or require disproportionate effort:

- where the processing is carried out for **archiving** purposes in the public interest, for **scientific** or **historical research** purposes or for **statistical** purposes;
- where the provision of such information is likely to **render impossible** or **seriously impair** the **achievement of the objectives of the processing**.

In both cases, the data controller must nevertheless **take appropriate measures** to protect the rights and freedoms and legitimate interests of the data subject, including by making the information publicly available.

2nd situation: obtaining or communicating the information is expressly provided for by the **legislation or regulations in force**, in application of **international commitments** enforced in the Principality offering comparable guarantees;

3rd situation: the data controller is bound by a **legal obligation of secrecy**;

Example : a doctor is bound by professional secrecy with regard to medical information provided to him by his patients

4th situation : the data subject already has this information, whether or not the data have been collected directly from him or her.

When should this information be provided?

Article 11 of Law no. 1.565 of December 3, 2024 states that when personal data are collected **directly from** the data subject, information must be provided **at the time the data are obtained**.

Where personal data are **not collected directly from** the data subject, the following time limits apply:

- **within a reasonable time** after obtaining the personal data, but **not exceeding one month**, having regard to the particular circumstances in which the data are processed;
- if the personal data are to be used for the purposes of communicating with the data subject, **at the latest at the time of the first communication** with the data subject;
- if it is envisaged to communicate **the information to another recipient**, at the latest when the personal data **are communicated for the first time**.

How should the information be provided?

The information provided must be:

- **concise, intelligible** and easily **accessible**;
- in **clear** and **simple** terms;
- free of charge;
- in **writing** or by any **other appropriate**

Concise, intelligible and easily accessible

The information must be presented and communicated in an **effective and succinct** manner in order to avoid drowning the data subjects.

This information must be **clearly differentiated** from other non-privacy-related information such as contractual clauses or general conditions of use.



In practice, **to avoid excessive information**, the data controller can provide **at least the most important information**, such as its identity, the purpose of the processing, whether replies are mandatory or optional and the rights of individuals, **and then refer to a privacy policy/information notice containing all the other mandatory information**.

The information must be understandable to the majority of the target audience.

Finally, the data subject **should not have to search for the information**, but should be able to access it immediately.

Example : a website's confidentiality policy must be accessible on every page of the site in a dedicated section. It must reflect the reality of processing and not be too generic. The font, including its size and colour, should not make it difficult to read. This policy must also be understood by the majority of residents in the Principality, and therefore be available in French.

In clear and simple terms

Information should be provided **as simply as possible**, avoiding complex sentences and linguistic structures.

It should not be formulated in vague, abstract or ambiguous terms, or be open to different interpretations.

Terms that are too legal, technical or specialized are not recommended.



Particular attention must be paid to information intended for minors. The data controller must ensure that the vocabulary, tone and style of language are appropriate for a young audience. For example, much simpler words or illustrations may be used.

Free of charge

The data controller may not demand payment from data subjects for the provision of information relating to the processing of their data.

This information **cannot therefore be made conditional on financial transactions**, such as the purchase of goods or services.

It is important to note that in the event of a request that is **manifestly unfounded or abusive, particularly due to its repetitive nature**, the data controller may either:

- demand the **payment of reasonable charges** which take into account the **administrative costs incurred** in providing the information, making the communications or taking the measures requested;
- refuse to comply with the request.



It will be up to the data controller to demonstrate that the request is manifestly unfounded or excessive.

In writing or by any appropriate means

Information should ideally be provided in writing.

However, if the data subject so requests, the information may be provided **orally, provided that the identity of the data subject is demonstrated by other means.**

In addition to electronic means, data controllers may use any appropriate means, including the use of graphics, computer graphics, flowcharts and even cartoons when the information is aimed at minors in particular.

The most important thing is that the method chosen to communicate the information must be **adapted to the particular circumstances of the situation.**

Examples:

- a sign posted at each entrance to an establishment for a video surveillance system
- a note on the access badge issuance document

What is the penalty for failure to comply with the obligation to provide information?

Article 54 of Law no. 1.565 of December 3, 2024 stipulates that failure to comply with the obligations relating to the information to be provided to the data subjects is punishable by an administrative fine of up to **10,000,000 Euros or, in the case of a company, up to 4% of the previous year's total worldwide annual revenue, whichever is the highest.**