

The consent of data subjects

The consent of the data subjects is **one of the 6 legal bases**, identified by article 5 of Law no. 1.565 of December 3, 2024 allowing **personal data to be processed in a lawful manner**.

Article 2 of this law defines consent 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 ».



To be valid, the **agreement given** by the data subject must therefore **meet several conditions**, namely, it must be:

- **freely given,**
- **specific,**
- **informed,** and
- **unambiguous.**

Conditions of consent

Freely given consent

This first condition implies that the data subject must be able to **make a real choice** regarding the processing of his or her data. This means that they must **not be forced or influenced** in their choice. Nor should they suffer any negative consequences if they do not give their consent.

In its guidelines on consent, adopted on May 4, 2020, the article 29 Working Group (Art.29 WP)¹ identifies a number of situations in which **it is presumed that consent is not free**. These include:

- The **manifest imbalance of power between the data subject and the data controller**, particularly when the latter is a Public Authority or an employer.

Indeed, when the data subject has to consent to a **processing operation set up by a Public Authority**, which is therefore acting as data controller, he or she enjoys **limited freedom of choice**, since there is **no alternative to accepting** the processing operation envisaged by the said Authority. The G29 therefore suggests that Public Authorities use more appropriate legal bases, namely the existence of a legal obligation or the pursuit of a public interest mission.

The existence of a **relationship of subordination** arising from a contract of employment concluded between the employer and his/her employee also leads to an **imbalance** in the case of data processing based on consent. Employees may fear that they **will be penalized if they refuse**, which prevents them from exercising a genuine choice.

As a result, employers, as data controllers, can very rarely obtain consent from their employees to process their data. Such processing must be justified by another legal basis, such as the existence of a legal obligation or the fulfilment of a legitimate interest pursued by the data controller.

Example: the installation of a video surveillance system in a store cannot be justified by the consent of employees as they are in a relationship of subordination to their employer and will not be in a position to consent freely. On the other hand, such a system could be justified by the data controller's legitimate interest in ensuring the safety of people and property.



¹ Independent European Union advisory board which dealt with issues relating to the protection of privacy and personal data until May 25, 2018 before being replaced by the European Data Protection Board.

- **Consent coupled with acceptance of general terms and conditions** or where the **provision of a contract or service is subject to a request for consent** to the processing of personal data not necessary for the performance of that contract or service.

In such a case, the appropriate legal basis will be the performance of a contract, provided that the data requested are indeed **necessary** for the performance of the said contract.

Example : communication by the buyer of his/her postal address for the delivery of the goods he/she ordered



- The **detriment suffered in the event of refusal to give consent**.

The data subject must be able to **refuse to give consent at any time** in order to express genuine freedom of choice. Consequently, any deception, intimidation, coercion or significant negative consequences if a data subject does not consent will invalidate said consent.

Example of unrestricted consent: a merchant site uses a checkbox to obtain the consent of its customers to use their email address for commercial prospecting purposes

Examples of non-voluntary consent:

- a merchant site informs Internet users that they cannot place an order without consenting to the processing of their email address for commercial prospecting purposes
- consent is presented as a non-negotiable part of the general conditions of use

Specific consent

Consent must be **specific to the purpose** of the processing. Consequently, when the processing involves **several purposes**, consent must be obtained **independently for each purpose**. This is referred to as **separate** consent for each purpose.

The purpose must be described **clearly** and in **unambiguous** terms. To this end, the Art.29 WP suggests referring to the « *reasonable expectations of an average data subject* ».

This specificity criterion enables data subjects to retain a certain **degree of control** over their data. It constitutes a **guarantee against the use of personal data** collected for **purposes far removed** from those initially listed, and thus prevents the data from being misappropriated.

When processing operations need to be added or modified, **consent must again be sought** from the data subject, except in cases where another legal basis appears to be more appropriate.

Example of specific consent: a merchant site collects their customer's email address in order to send them updates on the processing of their order and also for commercial prospecting. Two checkboxes are provided for each of these purposes and the customers can therefore accept the first one « *sending updates relating to the processing of their order* » and refuse the second one « *sending commercial prospecting* ».

Example of non-specific consent: a merchant site wishing to collect an email address in order to « *manage customer relations* » does not constitute specific consent, as this term encompasses several very distinct purposes.

Informed consent

Before the data subject makes a choice, the data controller must provide him or her with **certain information** listed in article 11 of Law no. 1.565 of December 3, 2024. This includes in particular:

- **the identity and professional details of the data controller**, and where applicable, its **representative** in Monaco;
- the **categories of personal data** concerned;
- the processing **purposes** and its legal bases;
- the **period for which** the data are intended to be stored or, if not possible, the criteria used to determine that period;
- the **recipients or categories of recipients** to whom the data are disclosed.

This information not only enables the data controller to comply with the **principle of transparency** required by law, but also enables the data subject to become aware of the use made of his/her data and to appreciate the consequences of his/her consent, thus enabling him/her to make an **informed choice**.

Information must be provided in a **clear, accessible way**, and be **adapted** to the intended recipients (data subjects). In order to adapt this information, the data controller must first determine the categories of data subjects and then consider the appropriate media.



The data controller must therefore use terms that can be **understood by as many people as possible**, with **particular attention** paid to the terms used when addressing **minors**.

Information can be provided **orally or in writing**, as well as in **audio or video messages**.



The information required to obtain valid consent is not considered accessible when provided in general terms and conditions of sale, as it is **not clearly differentiated** from other non-privacy-related information.

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

Example of informed consent: a company processes data on the basis of consent. It provides the data subject with most of the necessary information concerning the data controller and the processing operations. However, it fails to provide a list of the personal data processed. The company indicates only the categories of data concerned, without detailing their content. The consent obtained by the company is valid, since the data controller only needs to communicate the categories of data concerned by the processing.

Example of uninformed consent: a company processes data using consent as its legal basis. It provides the data subject with the following information: the identity of the data controller, a list of the categories of data that will be processed, the purposes pursued, the existence of a right to withdraw consent, and the absence of recourse to an automated decision. However, it fails to mention the existence of a data transfer to another company located in the United States for order processing purposes. As a result, the consent obtained is not informed, since the data subject was unaware at the time of collection that the data controller was carrying out such a transfer.



The data subject must be informed of any transfer outside the Principality. Moreover, if the data is transferred to a country that does not provide an adequate level of protection, the data controller must also inform the data subject of the **safeguards in place**.

Unambiguous consent

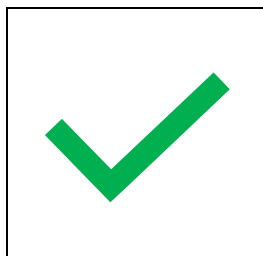
Consent must be given by an **oral** or **written** declaration by the data subject, or be the result of a **clear affirmative** act. There must be no reasonable doubt as to the data subject's wish to consent to the processing of his/her data.

Silence or inaction on the part of the data subject therefore does not constitute **valid consent** within the meaning of data protection legislation, as consent is not unambiguous.

Example of unambiguous consent : the use of a checkbox when consulting a website, clearly indicating that the data subject agrees to his or her email address being used to receive promotional information.

Examples of non-unambiguous consent :

- the use of a pre-ticked box, since the data subject has not taken a deliberate action to consent
- a statement in the privacy policy informing the data subject that, by continuing to use the service, he or she consents to the processing of his or her personal data
- global acceptance of the general terms and conditions, with no action required on the part of the Internet user



Special case of consent to the processing of sensitive data: explicit consent

In addition to this « *classic* » consent provided for in article 6 of Law no. 1.565 of December 3, 2024, article 7 of the same law provides for **reinforced** consent when a data controller relies on the consent of the data subject to process sensitive data.

What are considered sensitive data?

Article 2 of Law no. 1.565 of December 3, 2024 defines sensitive data as:

« personal data revealing, directly or indirectly, political opinions or affiliations, racial or ethnic origins, religious or philosophical beliefs, trade-union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person or data concerning the health, sex life or sexual orientation of a natural person »

Sensitive data constitute therefore a **special category** of personal data that are highly private.

In principle, the processing of sensitive data is prohibited by law due to the **high risk** of breaches of privacy. However, there are exceptions to this prohibition, including one based on the **explicit consent** of the data subject.

This explicit consent implies that the consent is of course **given freely, specific, informed and unambiguous**, but also that it is **affirmed in a clear statement**.

It should therefore no longer be possible to infer consent solely from the actions of the data subject, but rather it should be characterized by **clearly expressed words**.

This can be done in a number of ways, such as:

- a written and signed declaration
- an electronic form to be completed
- an e-mail to be sent back
- the use of an electronic signature
- a telephone conversation, provided that a specific request for confirmation from the data subject is formulated in a clear and comprehensible manner (e.g. pressing a button or giving oral confirmation)

Example of explicit consent: a cosmetic surgery clinic asks for a patient's explicit consent to transfer his medical file to another doctor in order to obtain a second opinion on the patient's condition. The medical file is in electronic form and includes health data, *i.e.* sensitive data within the meaning of the Law. Before any file transfer, the clinic asks the patient to give his explicit consent by electronically signing the agreement.

Example of non-explicit consent: a hospital wants to invite some of its patients to take part in an observational research. The investigating doctor sees them in consultation to explain the

purposes of the research and, once the patients have given their oral consent, he gives them an information note explaining the entire research process. This consent is not explicit because, in addition to the information note, the doctor must also get the patients to sign a consent form which summarizes the content of the information note. This form must also include boxes to be ticked if additional research or sampling is planned, so that the data subjects can give their express consent.

Withdrawal of consent

The data subject must be able to withdraw consent **at any time**.

The data controllers must therefore inform the data subject **of the existence of the right to withdraw consent at the very moment that consent is obtained**. They must also indicate the **procedure to be followed** to exercise this right of withdrawal.



Withdrawing consent must be as easy as giving it

Consequently, if this right is exercised, the data subject **does not have to give reasons for his or her choice**.

Furthermore, the data subject must **not suffer any prejudice as a result of withdrawing consent**, other than the cessation of benefits that may have resulted from the use of the data to which he or she had initially consented.



Example of a compliant withdrawal: the data subject had given consent to a merchant site to receive commercial prospecting emails. Due to the excessive volume of emails received, the data subject wishes to unsubscribe from this functionality. An « *Unsubscribe* » button appears at the bottom of each email and when the person clicks on it, he/she redirected to a page indicating that his/her opt-out choice has been taken into account.

Examples of non-compliant withdrawals:

- the data controller asks the data subject to state the reasons why he or she wishes to exercise his or her right of withdrawal
- data subjects who have given their consent online must, in order to withdraw it, call a telephone number indicated on the platform during working hours.

It is important to note that withdrawal of consent does not compromise the lawfulness of the processing carried out prior to such withdrawal.

On the other hand, once consent has been withdrawn, it is no longer possible to process personal data on this basis.

The data subject may therefore request the controller to delete or erase his/her personal data.

Proof of consent

Pursuant to the first paragraph of article 6 of Law no. 1.565 of December 3, 2024, the data controller must be able to **demonstrate that the data subject has given his/her consent** to the processing of his/her personal data.

This obligation of proof on the part of the data controller applies for **as long as the processing activity in question continues**.



Therefore, once the purpose of the processing has been achieved, proof of consent should be kept no longer than :

- the time required to comply with a **legal obligation**, or
- the time required to **establish, exercise or defend legal claims**.

Proof of consent must relate to :

- **the existence of consent**; and
- **the validity of consent** *i.e.* that the data controller has complied with the conditions set out in the first paragraph of Article 6 of the Law.



The Law does not specify how long consent is valid. The Article 29 Working Group therefore recommends that consent be **renewed** at **appropriate intervals**, ensuring that the data subject remains well informed.



Nor does the law specify how this obligation is to be met. As a result, data controllers are free to implement **whatever methods they deem appropriate**. However, they must ensure that these methods **do not lead to excessive additional processing**.

Example of proof of consent: Data & U manages a website. It offers Internet users the option of subscribing to a newsletter. To do so, they simply need to enter their email address. However, to ensure that the request is taken into account, the company automatically sends an email to the address indicated, containing a link that the person must click on for the subscription to become effective.

The consent of minors

Specific rules apply to minors **under the age of 15**, to whom, as **vulnerable persons**, the data controller must pay particular attention in the case of a **direct offer of an information society service**.

What do we mean by information society services?

The number 20 of article 2 defines an information society service as « *any service, whether or not for consideration, provided at a distance and without the parties being simultaneously present, by electronic means and at the individual request of a recipient of services* ».

Examples :

- ordering clothes on a merchant site
- online subscription to an electronic magazine

The data controller must draft the information notice in **clear and simple terms** so that the information can be **easily understood by the minor**.

Example: the data controller may use images or animated videos to explain the data processing to the minor.

Law no. 1.565 of December 3, 2024 also specifies that minors **under the age of 15 may not, on their own, give their consent** to the processing of their personal data. Indeed, for consent to be valid, the data controller must ensure that it has been **given** by the minor with the authorization of the person or persons exercising parental authority.

The data subject (or the person(s) exercising parental authority over the minor under the age of 15) has/have the right to withdraw consent **at any time**.

Finally, there are exceptions to the need for joint consent, in particular for preventive or advisory services offered directly to the minor. In such cases, the minor may consent alone.

What is the penalty for failing to verify that consent has been obtained?

Article 53 of Law no. 1.565 of 3 December 2024 provides that failure to comply with the obligation to verify that consent has been obtained is punishable by administrative fine of up to **5,000,000 Euros or, for companies, up to 2% of the total worldwide annual turnover of the previous financial year, whichever amount is the highest**.