Consent under GDPR: When to act and what to do

EDPB European Data Protection Board

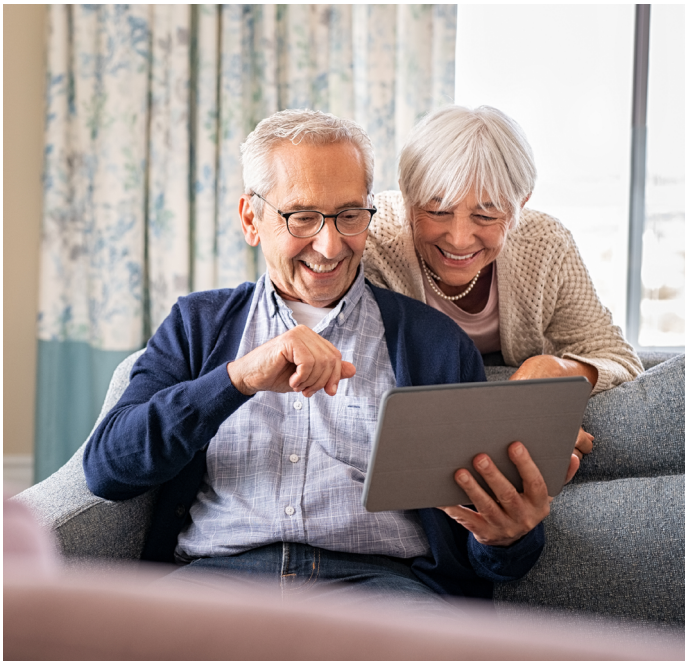
May 2026

Consent is one of the lawful bases for processing personal data under the General Data Protection Regulation (GDPR), providing individuals with control over the processing of their personal data.

For consent to be valid, it must meet the requirements set out in the GDPR which ensure that individuals are empowered to make informed decisions about the processing of their personal data. If the requirements for valid consent are not met, the processing activity cannot rely on this legal basis.

The goal is to ensure that individuals are offered a **genuine choice and control**. If an individual feels compelled to consent or will endure negative consequences if they do not, the consent is invalid.

The EDPB Guidelines on consent provide guidance on the validity of consent, the conditions for obtaining it, and discuss specific aspects in relation to children's data and scientific research.



The 4 elements of valid consent

Your checklist for validity. For consent to be valid, it must meet four cumulative criteria. If any of these are missing, the consent is invalid.

Element	What you need to know
1. Freely given	The individual must have **a real choice and control**. Consent is not free if it is bundled with non-negotiable terms (conditionality) or if there is an imbalance of power (e.g., employer/employee). Organisations need to demonstrate that it is possible to refuse or withdraw consent without detriment.
2. Specific	Consent must be granular. If you process data for multiple purposes, you should propose separate consents as individuals should be free to choose which purpose they accept. Vague purposes like "improving user experience" are not specific enough.

Element	What you need to know
3. Informed	You must provide clear information before consent is given. This includes the data controller's identity, the purpose of processing, the type of data, and the right to withdraw consent.
4. Unambiguous	Consent requires a clear affirmative action. Silence, pre-ticked boxes, or inactivity do not constitute consent.

Obtaining explicit consent

In some sensitive situations, organisations must get very clear and direct permission from an individual before using their data. This is called **explicit consent**.

It is required especially when processing sensitive personal data (like health, religion, biometric data), transferring data to non-European countries without adequate safeguards, and in the case of automated individual decision-making (like profiling).

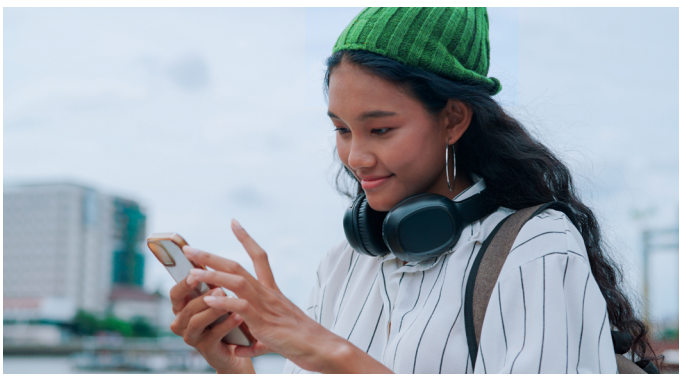
For the consent to be explicit, individuals must give an express statement of consent. An obvious way to make sure consent is explicit is to expressly confirm it in a written statement.

The law does not always require a signed paper document, but the organisation must be able to prove that the individual clearly agreed. Other ways to give explicit consent include filling in an online form, sending an email confirming consent, uploading a scanned document with the signature of the individual, and confirming during a phone call (for example, by pressing a button or clearly saying yes).

Withdrawal of consent

Individuals have the right to withdraw consent at any time.

- **The rule:** Withdrawing consent must be **as easy as giving it.** If consent was given with one click, it should be possible to withdraw it as easily.
- **Consequence:** If consent is withdrawn, you must stop the processing actions concerned.



Children (information society services)

When offering information society services directly to a child, specific rules apply.

- **Age of consent:** Processing is lawful if the child is at least 16 years old (countries may lower this age, but not below 13).
- **Parental authorisation:** If the child is below the age limit, consent must be given or authorised by the holder of parental responsibility. You must make reasonable efforts to verify that consent is given or authorised by them, taking into consideration available technology.

Practical examples

Here are specific scenarios illustrating how to apply these rules:

Example

(section 3.1, paragraph 15, page 8)

Context: A mobile app for photo editing asks users to activate GPS localisation and consent to behavioural advertising. Neither is necessary for the photo editing functionality.

What to do: The data controller must not make the core service (photo editing) conditional on consent for unnecessary data (GPS/Ads). To fix this, the app should allow users to access the editing features even if they refuse GPS or ad tracking.

Example

(section 3.4, paragraph 86, page 19)

Context: A website relies on users simply scrolling through a webpage as an indication of consent.

What to do: The data controller cannot rely on scrolling or swiping through a page as it is not a "clear affirmative action". Instead, they must implement an unambiguous action, such as ticking a box or a specific "swipe this bar to agree to the use of information X for purpose Y" motion (where the motion clearly signifies agreement to a specific request).

Example

(section 3.1.2, paragraph 40, page 12)

Context: A website uses a "cookie wall" that blocks content visibility unless the user clicks "Accept cookies."

What to do: The individual is not presented with a genuine choice as the provision of the service relies on the individuals clicking the "Accept cookies" button, therefore, consent is not freely given, and this does not constitute valid consent.

Data controllers are responsible for demonstrating that valid consent was obtained. By ensuring consent is a genuine, informed choice, you build trust and ensure your processing is lawful.

This document provides a simplified overview of the guidelines. For more comprehensive legal explanations and examples, please consult the full guidelines.

Read the complete guidelines