Here is a simplified guide to the Legal Bases for Processing under the GDPR

Contents

Legal Basis for Processing under the GDPR

Article 6, Article 7, Article 8, Article 9 and Article 10.

The Six Lawful Bases for Processing:

To collect or use personal data legally, you cannot just "want" to do it. You must rely on one of six specific legal justifications (Article 6). If you cannot fit your processing into one of these boxes, you cannot collect the data.

You must identify and document one of these bases before you start processing data.

- **Consent:** The individual has given you clear, specific permission to process their data for a specific purpose.
- **Contract:** You need to process the data to fulfil a contract with the individual (e.g., you need their address to deliver goods they bought).
- **Legal Obligation:** You are required by law to process the data (e.g., keeping salary records for tax purposes).
- **Vital Interests:** It is a life-or-death situation (e.g., giving emergency medical data to a hospital to save someone's life).
- **Legitimate Interests:** You have a genuine business reason (like fraud prevention or network security), and this reason is not overridden by the individual's rights or freedoms.
- **Public Interest:** You are performing a task in the public interest or acting under official authority (usually applies to government bodies, not private companies).

Strict Rules for "Consent" (Article 7)

If you choose "Consent" as your legal basis, the bar is set very high. You must be able to prove you obtained it validly.

- **Freely Given:** The user must have a real choice. You cannot force them to consent or punish them if they say no.
- **Informed:** They must know exactly who you are and what you are doing with their data.
- **Specific:** You cannot ask for "blanket consent." You must ask for permission for each specific purpose.
- **Clear Affirmative Action:** The user must do something to consent (like ticking a box). You must also keep a record of this consent being given. Pre-ticked boxes are banned.
- **Easy Withdrawal:** You must tell them they can withdraw consent at any time, and if they do, you must stop processing immediately.

Processing Children's Data (Article 8)

There are extra protections for children, specifically regarding "Information Society Services" (apps, games, social media).

- **The Age Limit:** If the user is under 16 (some other EU member states have this as low as 13), you cannot accept their consent alone.
- **Parental Consent:** You must obtain consent from the holder of parental responsibility.
- **Verification:** You cannot just ask "Are you a parent?" You must take "reasonable steps" to verify that the person giving consent is actually the parent/guardian.
- **Plain Language:** Notices must be written simply enough for a child to understand.

"Special Category" Data (Article 9)

Some data is considered so sensitive that processing it is generally prohibited by default.

This includes data revealing:

- Racial or ethnic origin
- Political opinions, religious beliefs, or trade union membership
- Genetic or biometric data (used for ID purposes)
- Health data or sexual orientation

When can you process this?

You need a lawful basis from Article 6 PLUS a specific condition from Article 9, such as:

- **Explicit Consent:** The user gave a very clear, documented "yes" for this specific sensitive data.
- **Employment Law:** It is necessary for employment or social welfare obligations.
- **Vital Interests:** The person is physically or legally incapable of giving consent (e.g., they are unconscious).
- **Legal Claims:** You need it to defend yourself in court.

Criminal Convictions (Article 10)

Handling data about criminal records or security measures is heavily restricted.

- **Official Authority Only:** Generally, this can only be done under the control of official authority (like An Garda Síochána).
- **Authorised by Law:** Private organisations can only process this data if specific EU or Member State law authorises it and appropriate safeguards are in place. You cannot just rely on "Legitimate Interests" or standard "Consent" for this.

Here is an expanded guide on the five alternatives to "Consent." As an organisation, relying on these can often be more stable than Consent because individuals cannot just "withdraw" them as easily (though they may still have rights to object).

Contractual Necessity

When to use it: Use this when you have a contract with an individual (or are about to enter one) and you literally cannot do your job without their data.

The Rule: The processing must be necessary for the performance of a contract to which the individual is a party.

Practical Example: If you sell a product online, you need the customer's address to deliver it. You don't need their consent for the address. You need it to fulfil the contract of sale.

Constraint: You cannot use this for things that are "nice to have" but not essential to the contract (e.g., using that same address for marketing newsletters usually requires a different basis, like Consent).

Legal Obligation

When to use it: Use this when you have no choice because the law says you must process the data.

The Rule: The processing is necessary for compliance with a legal obligation.

Practical Example: You are required by tax laws to keep records of employee salaries for a certain number of years. Even if an employee asks you to delete their data, you can refuse because you have a legal obligation to keep it.

Constraint: This must be a statutory obligation (EU or National law), not just a contractual obligation to a third party or your own company policy.

Vital Interests

When to use it: This is the "Emergency Only" basis. It applies to life-or-death situations.

The Rule: The processing is necessary to protect the vital interests of the data subject or another person.

Practical Example: If a visitor to your office collapses and is unconscious, you might disclose their medical allergies (if known) to the paramedics. You don't need to wake them up to get consent because their life (vital interest) is at risk.

Constraint: You generally cannot use this for large-scale data processing or health data unless it is truly a medical emergency.

Legitimate Interests

When to use it: This is the most flexible basis, often used for business activities like fraud prevention, network security, or direct marketing. However, it requires a careful "Balancing Test".

The Rule: Processing is necessary for your legitimate interests (or those of a third party), UNLESS those interests are overridden by the individual's fundamental rights and freedoms.

The "Balancing Test": You must weigh your benefit against the user's privacy:

> **Your side:** "We need to process IP addresses to stop hackers attacking our website." (This is a strong legitimate interest).
>
> **Their side:** "Does this hurt the user's privacy?" (Likely minimal impact).
>
> **Result:** You can probably proceed.

Constraint: If the processing would be unexpected, cause harm, or if the individual is a child, their rights likely override your interests. You must document this assessment.

Public Interest / Official Authority

When to use it: This is primarily for public authorities (like schools, hospitals, police, or councils) performing their official duties.

The Rule: The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in you.

Practical Example: A local council collecting data to organise bin collection or a tax authority collecting income data.

Constraint: Private companies rarely use this unless they are contracted to carry out specific public tasks (e.g., a private utility company maintaining the water supply).

"Soft Opt-in" – What is it?

Usually, you need a person to actively say "Yes" (Consent) before you can send them marketing emails. The "Soft Opt-in" is a specific exception for existing customers. This comes from the ePrivacy Directive, which sits alongside the GDPR. It allows you to assume that because a customer bought something from you, they are likely happy to hear about similar products, provided you give them the chance to say "no."

The "Soft Opt-in" Checklist:

To use this legally, you must meet all four of the following criteria. If you fail on even one, you must ask for fresh Consent.

1. You obtained the data during a "Sale or Negotiation for a Sale"

   The Rule: You didn't buy a marketing list or scrape the data from the web. You got the details directly from the individual while they were buying a product or service from you.

   The "Negotiation" nuance: This also applies if they nearly bought something (e.g., they put items in a basket and entered their email but didn't click "pay," or they asked for a quote).

2. You are marketing "Similar Products or Services"

   The Rule: You can only market your own products that are relevant to what they bought.

   Example: If they bought a lawnmower, you could email them about grass seed. You cannot email them about online gambling or health insurance.

3. You gave them a chance to Opt-out when you collected the data

   The Rule: At the moment they handed over their email address (e.g., the checkout screen), you must have given them a clear opportunity to refuse marketing.

   Your Obligation: This is often an "unsubscribe" box or a clear statement saying, "We will send you updates, check here if you do not want this." If you hid this fact, you cannot use the soft opt-in.

4. You give them a chance to Opt-out in every single message

   The Rule: Every subsequent email must have a clear "Unsubscribe" link.

   GDPR Connection: This links directly to the Right to Object. The text states you "must stop processing personal data for direct marketing purposes as soon as you receive an objection". There are "no exemptions or grounds to refuse" this request.

Which Legal Basis is this?

When using the Soft Opt-in, you are not relying on Consent. You are relying on Legitimate Interests.

Why this matters: You do not need the "Clear affirmative action" (ticked box) required for Consent. Instead, you are arguing that your interest in growing your business is legitimate and does not override the customer's rights because they reasonably expect to hear from you after a purchase.