The GDPR provides the following rights of an individual:

The right to be informed

Article 13 and Article 14.

Your Obligation: You must be completely transparent about how you use personal data. You cannot collect data in secret; you must provide "fair processing information," typically through a Privacy Notice.

What to include: You must detail your identity and contact info (and that of your DPO), why you are processing the data and the legal basis for doing so, how long you will keep it, and who else will receive it. You must also list the users' rights, including their right to withdraw consent or lodge a complaint.

Format: The information must be concise, transparent, intelligible, easily accessible, and free of charge. It must be written in clear, plain language—especially if addressed to a child.

Timing:

- **Direct Collection:** If you got the data straight from the individual, give them this info at the time you collect it.
- **Indirect Collection:** If you got the data from elsewhere, you must inform the individual within a reasonable period (maximum one month), or at the point you first communicate with them or share the data with someone else.

The table below summarises the information you should supply to individuals where the personal data has been obtained either directly from the data subject or by another means.

Identity and contact details of the controller (and where applicable, the controller's representative) and the data protection officer.	The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences.
Any recipient or categories of recipients of the personal data.	Purpose of the processing and the legal basis for the processing.
The right to lodge a complaint with a supervisory authority.	The existence of each of data subject's rights.
Retention period or criteria used to determine the retention period.	Details of transfers to a different country and what safeguards apply.
The right to withdraw consent at any time, where relevant.	The legitimate interests of the controller or third party, where applicable.

If the personal data was obtained directly from the data subject, then you should provide them with the above information at the time you get the personal data.

The next table summarises the information you should supply to individuals where the personal data has not been obtained directly from the data subject.

The source the personal data originates from and whether it came from publicly accessible sources.	Categories of personal data.

The right of access (Subject Access Requests)

Article 15.

Your Obligation: You must allow individuals to verify that their data is being processed lawfully. If asked, you must confirm you are processing their data and provide a copy of it.

Deadlines: You must respond without delay, and at the latest within one month.

Extension: You can extend this by two months if the request is complex or numerous, but you must notify the individual within the first month and explain why.

Fees: You generally cannot charge a fee.

> ***Exception:*** You may charge a "reasonable fee" based on administrative costs only if the request is "manifestly unfounded or excessive" (e.g., repetitive) or for additional copies.

Verification: You must verify the identity of the requester using reasonable means before handing over data.

> **Suggested ways:**
>
> - Ask the individual to confirm details only they would know based on the data you already hold. Ask 2-3 specific questions:
> - "Please confirm the amount of your last transaction with us."
> - "What is the reference number on your most recent bill?"
> - "Please confirm the phone number we have on file for you."
> - Require the user to log in to their secure account area to submit the request.
> - If you must ask for photo ID, ask them to redact unnecessary information – e.g. “Please send a photo of your driving licence, but please black out your licence number and date of birth. We only need to see your name and photo”

Format: If the request is made electronically, you should provide the data in a commonly used electronic format.

The right to rectification

Article 16.

Your Obligation: You must correct inaccurate or incomplete personal data upon request.

Third Parties: If you have shared this data with other organisations, you must inform them of the correction if possible.

Deadlines: You have one month to comply. This can be extended by two months for complex requests, provided you notify the individual.

Refusal: If you decide not to take action, you must explain why and inform the individual of their right to complain to a supervisory authority.

The right to erasure ("Right to be Forgotten")

Article 17.

Your Obligation: You must delete personal data when there is no compelling reason to keep it. **BUT** this is not an absolute right. You are quite likely to refuse this one, as its scope is quite narrow.

When to delete: You must act if:

a) consent is withdrawn
b) the data is no longer needed for its original purpose
c) it was processed unlawfully
d) if there is a legal obligation to delete it

Special attention is required for data collected from children online.

Public Data: If you have made the data public (e.g., on a website), you must take reasonable steps to inform other controllers processing that data to erase links to or copies of it.

Exceptions: You can refuse deletion if the processing is necessary for freedom of expression, public health, contractual, legal obligations, or the defence of legal claims.

The right to restrict processing

Article 18.

Your Obligation: In specific circumstances, you must stop using the data but keep it stored. You can retain just enough info to ensure the restriction is respected in the future.

When to restrict: You must apply this if an individual contests the accuracy of data (while you verify it), if they object to processing (while you verify your legitimate grounds), or if the processing is unlawful but the individual prefers restriction over deletion.

Notification: You must inform any third parties you shared the data with about the restriction. You must also tell the individual before you lift the restriction.

The right to data portability

Article 20.

Your Obligation: You must allow individuals to obtain and reuse their data across different services by providing it in a format that allows easy transfer.

Format: Provide the data in a structured, commonly used, and machine-readable form (e.g., CSV files) so software can extract the data.

Scope: This applies only to data the individual provided to you, processed by automated means, based on consent or a contract.

Direct Transfer: If the individual asks and it is technically feasible, you should transfer the data directly to another organisation.

The right to object

Article 21.

Your Obligation: You must respect an individual's right to say "no" to processing in certain cases.

Direct Marketing: If an individual objects to direct marketing, you must stop immediately. There are no exemptions or grounds to refuse.

Legitimate Interests/Public Task: If they object to processing based on these grounds, you must stop unless you can demonstrate "compelling legitimate grounds" that override their rights, or if it is for legal claims.

Communication: You must explicitly bring this right to their attention at the point of first communication and in your privacy notice, keeping it separate from other information.

Rights in relation to automated decision making and profiling

Article 22.

Your Obligation: You must provide safeguards against potentially damaging decisions made solely by computers without human intervention.

The Right: Individuals can refuse to be subject to automated decisions that have legal or significant effects on them.

Safeguards: If you use automated decision-making, you must allow the individual to obtain human intervention, express their point of view, and obtain an explanation of the decision so they can challenge it.

Profiling: If you use profiling (analysing personal aspects like performance, health, or location), you must be transparent about the logic involved and the significance of the consequences. You must use appropriate mathematical procedures and secure the data to prevent errors or discrimination.