The GDPR provides the following rights of an individual:

The right to be informed

Article 13 and Article 14.

The right to be informed covers your responsibility to provide "fair processing information", normally by way of a privacy notice. You need to be absolutely transparent in how you are going to use personal data.

What information must be supplied?

The General Data Protection Regulation (GDPR) sets out the information that you should supply to an individual and when they should be informed of this information.

The information you supply is determined by whether or not you obtained the personal data directly from a data subject or not. Much of the information you should supply is consistent with previous responsibilities under the Data Protection Act 1988 (as amended in 2003), but there is some further information you are explicitly required to provide.

The information you supply about the processing of personal data must be:

- Concise, transparent, intelligible and easily accessible
- Written in clear and plain language, particularly if addressed to a child
- Provided free of charge

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.

In above two tables, If the personal data was not obtained from the data subject, then you should provide the data subject with the information within a reasonable period of having acquired the data (e.g. within one month). If you use the data to communicate with the data subject, then you should provide them with the information at the time you first communicate with them. If you are intending to share the personal data with another entity, then you should provide the data subject with the information **before** you share the personal data.

Finally you need to advise the data subject, at the time you are gathering the personal data, about whether the provision of personal data is part of a statutory or contractual requirement or obligation and the possible consequences of failing to provide the personal data.

The right of access

Article 15.

What information is an EU resident entitled to under the GDPR?

Under the GDPR, EU residents will have the right to obtain:

- Confirmation that their personal data are being processed
- Access to a copy of their personal data
- Any other supplementary information

What is the purpose of the right of access under GDPR?

The General Data Protection Regulation (GDPR) clarifies that the reason for allowing individuals to access their personal data is so that they are aware of and can verify the lawfulness of the processing and the accuracy of their data.

How long do I have to comply?

Previously under the Data Protection Act 1988/2003, you had to respond within 40 days of a subject access request. Under the GDPR information must be provided without delay and at the latest within one month of receipt of the request.

If the request is complex or numerous, then you will be able to extend the period of compliance by a further two months. In this case, you must notify the individual within one month of the receipt of the request and explain why the extension is necessary.

Can I charge a fee for dealing with a subject access request?

You must provide a copy of the data subject's personal data free of charge. The Data Protection Act (DPA) 1988/2003 had a fee of €6.35, but this has been removed under the GDPR.

If a request is manifestly unfounded or excessive and particularly if it is repetitive, then you may charge a "reasonable fee". This fee must be based on the legitimate administrative cost of providing the personal data.

You may also charge a reasonable fee to comply with requests for additional copies of the same information. This does **not** mean that you can charge for access requests that come at a later date.

What if the request is manifestly unfounded or excessive?

Where requests are manifestly unfounded or excessive, in particular because they are repetitive, you can:

- charge a reasonable fee taking into account the administrative costs of providing the information
  -OR-
- refuse to respond

Where you refuse to respond to a request, you must explain the reason why to the individual, informing them of their right to complain to the supervisory authority and to seek a legal remedy without undue delay and at the latest, within one month.

What about requests for large amounts of personal data?

Where you process a large volume of information about a data subject, the GDPR allows you to ask the individual to specify exactly what information the request relates to.

The GDPR does not introduce an exemption for requests that relate to large amounts of data, but it does allow you to consider whether the request is manifestly unfounded or excessive.

How should the information be provided?

You must first verify the identity of the person making the request, using “reasonable means”.

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

There is a new best practice suggestion introduced with the GDPR that, where possible, organisations should be able to provide secure remote access to a secure self-service system which would provide the individual with direct access to their personal data. This will not be appropriate for all organisations, and it will be up to each organisation to make that determination for themselves.

The right to obtain a copy of their information or to access personal data through a remotely accessed secure system should not adversely affect the rights and freedoms of others.

The right to rectification

Article 16.

When should personal data be rectified?

Individuals are entitled to have their personal data corrected if it is inaccurate or incomplete. If you have divulged the personal data in question to third parties, you must inform them of the correction where possible. You must also inform the data subject about the third parties to whom the data has been divulged where appropriate.

How long do I have to comply with a request for rectification?

You must respond within one month.

This can be extended by two months where the request for rectification is complex or numerous. In this case you must notify the data subject within one month of receipt of the request and explain why the extension is necessary.

Where you are not going to take action in response to a request for rectification, you must explain why you are doing so to the individual and inform them of their right to complain to the supervisory authority and to seek a legal remedy.

The right to erasure

Article 17.

The right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

When does the right to erasure apply?

The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data deleted and to prevent processing in the following situations:

- When the data subject withdraws consent.
- The personal data has to be deleted to comply with a legal obligation.
- The personal data was unlawfully processed. This is a breach of the GDPR.
- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected.
- When the individual objects to the processing and there is no superseding legitimate requirement to continue the processing.
- The personal data is processed in relation to the offer of "information society services" to a child.

Previously under the Data Protection Act 1988/2003, the right to erasure is limited to processing that causes unwarranted and substantial damage or distress.

Under the GDPR, there is no such threshold, but if the processing does cause damage or distress, this will likely make the case for deletion stronger.

When can I refuse to comply with a request for erasure?

There are some specific situations where the right to erasure does not apply and you can refuse to deal with such a request. The following are those reasons:

- To exercise the right of freedom of expression and information.
- For public health purposes in the public interest.
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority.
- The exercise or defence of legal claims.
- Archiving purposes in the public interest, for scientific research, for historical research or for statistical purposes.

How does the right to erasure apply to children's personal data?

There are some extra requirements when the request for erasure relates to a child's personal data. This reflects the GDPR greater emphasis on protection of such personal data, especially in online environments.

If you process the personal data of children, you should pay special attention to existing situations where a child has previously given consent to processing and they later request erasure of the data (regardless of their age at the time of the request). This is especially so for social networking sites and internet forums. This is mainly because a child may not have been fully aware of the risks involved in the processing of their personal data at the time they originally gave consent.

Do I have to tell other organisations about the erasure of personal data?

If you have divulged the personal data, that is the subject of the erasure request, to some third parties, you must inform them also about the request, unless it is impossible or involves disproportionate effort to do so.

The GDPR reinforces the right to erasure by clarifying that organisations in the online environment who place personal data into a public environment, should inform the other organisations who process the personal data to erase links to, copies or replication of the personal data in question.

While this might be challenging, if you process personal information online, for example on social networks, forums or websites, you must make every effort to comply with these conditions.

The right to restrict processing

Article 18.

Under the DPA 1988/2003, individuals have a right to 'block' or suppress processing of personal data. The restriction of processing under the GDPR is similar. When processing is restricted, you are permitted to store the personal data, but not further process it. You can retain just enough information about the individual to ensure that the restriction is respected in future.

When does the right to restrict processing apply?

You will be required to restrict the processing of personal data in the following circumstances:

- Where the data subject raises doubts as to the accuracy of their personal data, you will need to stop any further processing until you have verified the accuracy of the personal data.
- Where the data subject has objected to the processing, and you are considering whether your organisation's legitimate grounds override those of the individual. This, in the situation, where it was necessary for the performance of a public interest task or purpose of legitimate interests.
- If you no longer need to store the personal data but the data subject requires the personal data in order to establish, exercise or defend a legal claim.
- When processing is unlawful and the data subject does not wish to have the personal data deleted, but opts for its processing to be restricted instead.

You may need to update your procedures to ensure that they meet the requirements to restrict processing as outlined above.

If you have divulged the personal data in question to third parties, you must also notify them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

You must notify the data subject(s) if and when you decide to lift a restriction on processing.

The right to data portability

Article 20.

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

When does the right to data portability apply?

The right to data portability only applies:

- To personal data the data subject has provided to a data controller.
- Where the processing is based on the data subject's consent or for the performance of a contract.
- When processing is carried out by automated methods.

How do I comply?

You must provide the personal data in a structured, widely used and machine readable form. One of the most commonly used, structured format is a CSV files. Machine readable means that the information is structured such that software can extract specific elements of the data. This enables ease of transfer to another organisation.

If the data subject requests it, you may be obliged to transfer their personal data directly to a third party organisation, if it is technically feasible. You are not, however, required to change your own processing systems to enable a direct interface with third-party systems.

If the personal data concerns more than one data subject, you must consider whether providing the information would prejudice the rights of any other data subject.

The personal data must be provided free of charge.

How long do I have to comply?

You must respond without undue delay, and at the most, within one month.

This can be extended by two months where the request is complex or you receive a number of requests. You must however inform the data subject within one month of the receipt of the request and explain why the extension is necessary.

Where you are decide not to take action in response to a request, you must explain why to the data subject, informing them of their right to complain to the supervisory authority and to a legal remedy without undue delay and at the latest within one month.

The right to object

Article 21.

Individuals have the right to object to:

- Processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling).
- Direct marketing (including profiling).
- Processing for purposes of scientific/historical research and statistics.

If you process personal data for the performance of a legal task or your organisation's legitimate interests:

Data subjects must have an objection on "grounds relating to his or her particular situation".

You must stop processing the personal data unless:

- You can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the data subject.
- The processing is for the establishment, exercise or defence of legal claims.

You must inform data subjects of their right to object "at the point of first communication" and in your privacy notice. This must be "explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information".

If you process personal data for research purposes:

Data subjects must have "grounds relating to his or her particular situation" in order to exercise their right to object to processing for research purposes.

If you are conducting research where the processing of personal data is necessary for the performance of a public interest task, you are not required to comply with an objection to the processing.

If you process personal data for direct marketing purposes:

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.

You must deal with an objection to processing for direct marketing at any time of day or night and no charge may be levied.

You must inform data subjects of their right to object "at the point of first communication" and in your privacy notice. This must be "explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information".

If your processing activities fall into any of the above categories and are carried out online:

You must offer a way for data subjects to object online.

Rights in relation to automated decision making and profiling

Article 22.

The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention. Study your processing operations and see if any of them use automated decision making. If they do, then check your procedures around this decision making to ensure that they deal with the requirements of the GDPR.

When does the right apply?

Data Subjects have the right not to be subject to a decision when:

- It is based on automated processing.
- It produces a legal effect or a similarly significant effect on the data subject.

You must ensure that data subjects are able to, obtain human intervention, express their point of view and obtain an explanation of the decision, such that they can challenge it.

Does the right apply to all automated decisions?

No. The right does not apply if the decision:

- Is necessary for entering into or performance of a contract between your organisation and the data subject.
- Is authorised by law (e.g. for the purposes of fraud or tax evasion prevention).
- Based on explicit consent from the data subject[§].

Furthermore, the right does not apply when a decision does not have a legal or similarly significant effect on someone.

[§] Article 9(2)

Does the GDPR say anything else about profiling?

The GDPR defines profiling as any form of automated processing intended to evaluate certain personal aspects of a data subject, in particular to analyse or predict their:

- Performance at work.
- Economic situation.
- Health.
- Personal preferences.
- Reliability.
- Behaviour.
- Location.
- Movements.

When processing personal data for profiling purposes, you must ensure that appropriate safeguards are in place:

- Ensure processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the envisaged consequences.
- Use appropriate mathematical or statistical procedures for the profiling.
- Implement appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.
- Secure personal data in a way that is proportionate to the risk to the interests and rights of the data subject and prevents discriminatory effects.

Automated decisions taken for the purposes listed in Article 9(2) must not concern a child or be based on the processing of special categories of data. That is unless:

- You have the explicit consent of the data subject
  -OR-
- The processing is necessary for reasons of substantial public interest on the basis of EU or individual Member State law. This must be proportionate to the aim pursued, respect the essence of the right to data protection and provide suitable and specific measures to safeguard fundamental rights and the interests of the data subject.