

What GDPR means for individuals

Up to this point we have focused on the implications of GDPR for companies and organisations, and it is vital to understand its impact on individuals.

The legislation provides individuals with eight rights for accessing their personal data. These are as follows:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and processing

These rights should be viewed positively for both companies and individuals, as it grants greater levels of control to both parties. Companies deal with informed customers who understand what they have signed up for, and individuals can make the right decisions from a position of knowledge.

Let's now run through these rights and take a closer look...

The right to be informed

Individuals have access to how their personal data is being processed, and all information you supply should be:

- concise, transparent, intelligible and easily accessible;
- written in clear and plain language, particularly if addressed to a child; and
- free of charge.

Example

An individual asks a digital agency who are running an email campaign what personal data they hold, and what platform is being used to distribute the emails (eg Mailchimp, Campaign Monitor, etc).

The digital agency must provide this information in an accessible way.

Disclaimer

This guide does not constitute legal advice or legal analysis. Organisations may still need to seek independent legal advice when developing their own processes, or when dealing with specific issues.

The right of access

Individuals have the right to access any personal data held about them by a company / organisation, and must be provided free or charge.

Companies can charge a 'reasonable fee' if the demands are excessive, unfounded or repetitive.

Data must be provided within **one month** of the request being made.

Example

An individual attended a university open day in 2012, but are still receiving email updates about future events.

As they have now graduated this is no longer relevant, so they make a request to see what personal data is stored.

The university marketing team must provide the information within the time frame.

The right to rectification

Individuals can request that personal data be rectified if they believe it to be inaccurate or incomplete.

Amendments must be made within **one month** of the request being made.

This deadline can be extended to **two months** if the process of rectification is complex.

Example

An individual is sent a marketing brochure featuring an incorrect middle name, and includes the wrong job title. They make a request to the company who sent out the brochure to rectify the personal data.

The company must comply with this request within the time frame.

Disclaimer

This guide does not constitute legal advice or legal analysis. Organisations may still need to seek independent legal advice when developing their own processes, or when dealing with specific issues.

The right to erasure

This is often called ‘the right to be forgotten.’ Individuals have the right to request personal data be removed if there is no compelling reason for it to be processed.

Example

An individual posted some slightly embarrassing photos of themselves on holiday aged 17 to social media platforms. They are now working in medicine, and feel this is not appropriate professionally, and request that the photos be removed.

The social media platforms must remove the images.

The right to restrict processing

Individuals have the right to block or restrict processing of personal data.

Companies can still store personal data but are not permitted to further process it.

You can store enough personal data to identify an individual and prevent future processing of their data.

Example

An individual receives a targeted social media advertisement for a research project about single people. They do not wish to take part, or have their relationship status used in this way, and use their right to restrict processing by contacting the agency who ran the ad.

The agency must comply and prevent this individual’s personal data from being processed in future campaigns.

The right to data portability

Individuals should have access to obtain and reuse their personal data across different services.

Moving personal data should be a simple, secure and safe process with a focus on usability.

Example

An individual has completed several online learning courses and CPD modules, and these are recorded on a popular learning platform website as records of achievement.

Disclaimer

This guide does not constitute legal advice or legal analysis. Organisations may still need to seek independent legal advice when developing their own processes, or when dealing with specific issues.

They want to use this data on their personal blog, and make a request to the website owners who provide it in a usable format (eg XML feed or HTML5 widget).

The right to object

Individuals have the right to object to personal data being used for:

- Profiling of individuals
- Direct marketing and targeted advertising
- Processing of personal data for research, surveys and historical studies

Example

An individual has discovered that their purchase history at an online retailer is being used to recommend products and services they object to (eg dating and gambling websites). They make a request to the online retailer for their personal data not to be used in this way.

The online retailer must comply with this request.

Rights in relation to automated decision making and processing

This relates to where personal data is being processed without human input (eg AI and algorithmic decision making).

Where profiles created using personal data form part of an automated decision making process individuals must be fully informed.

Example

Whenever automated decision making is used to process personal data companies must provide transparency wherever possible, and introduce simple ways of including human interaction and scope for challenging of decisions.

An example of this might be an individual who was refused a personal loan based on erroneous credit score information. They have the right to challenge this decision, and request information about the process.

Disclaimer

This guide does not constitute legal advice or legal analysis. Organisations may still need to seek independent legal advice when developing their own processes, or when dealing with specific issues.

Protecting children

GDPR includes new safeguards to protect children and generally will require explicit parental consent for online services aimed at children that process personal data.

Some EU member states may permit this to be a lower age, although it cannot be below the age of 13.

IT security and privacy

New guidelines are in place to protect individuals against the loss and misuse of personal data.

There are three main requirements:

- The Information Commissioner's Office must be informed of any data breaches within 72 hours of the incident happening.
- Any major IT projects may require a [Data Protection Impact Assessment \(DPIA\)](#) to mitigate the risks of potential data loss.
- All IT projects follow a [privacy by design methodology](#).

Using cloud-based services

The GDPR does permit the use of cloud-based services (Google Drive, Amazon Web Services, etc). If the services are US-based it is vital to ensure they are part of the [Privacy Shield Framework](#). This certifies that personal data is managed and processed to GDPR standards.

Disclaimer

This guide does not constitute legal advice or legal analysis. Organisations may still need to seek independent legal advice when developing their own processes, or when dealing with specific issues.