



The GDPR


What's it all about?


The General Data Protection Regulation is the biggest change to data protection laws in more than two decades, affecting everyone living in the EU. It came into effect in May 2018 to give people more control over how their personal data is handled.


Here are the seven key principles of the GDPR:


 **Lawfulness, fairness and transparency**
As a “controller” holding people’s data, we must identify valid grounds, known as a “lawful basis”, for collecting and using it. We must use personal data in a way that is fair – and be open and honest about how we use it.


 **Purpose limitation**
We must be clear about what our purposes for processing personal data are from the start and specify them in a privacy document for you to see.

 **Data minimisation**
We must ensure the personal data we process is adequate, relevant and limited to what is necessary – we do not hold more than we need to.

 **Accuracy**
We promise to take all reasonable steps to ensure the personal data we hold is not incorrect or misleading. If someone discovers it is incorrect or misleading, we must take reasonable steps to correct it as soon as possible.

 **Storage limitation**
We must not keep personal data for longer than we need to. We are required to justify how long we keep personal data and have a policy setting standard retention periods.

 **Security**
We must ensure that we have appropriate security measures in place to protect the personal data we hold. This is the GDPR’s “integrity and confidentiality” principle.

 **Accountability**
The accountability principle requires us to take responsibility for what we do with personal data. We have appropriate measures and records in place to be able to demonstrate our compliance.

Your rights



The right to be informed

You have the right to be told about the collection and use of your personal data, and with whom it will be shared. Privacy details must be provided whenever it is collected.



The right of access

You have the right to access your personal data (commonly referred to as subject access) and can make a request verbally or in writing.



The right to rectification

You have the right to have inaccurate personal data rectified, or completed if incomplete. Requests can be made verbally or in writing.



The right to erasure

You have the right to have your personal data erased, known as the Right to be Forgotten. Again, you can make a request for erasure verbally or in writing.



The right to restrict processing

You have the right to request the restriction of your data in certain circumstances. When processing is restricted, organisations are allowed to store the data but not use it.



The right to data portability

You have the right to obtain and reuse your data across different services. You must be able to move or copy personal data easily from one IT environment to another.



The right to object

You have the right to object to the processing of your personal data in certain circumstances, including to stop your details being used for direct marketing.



Rights over automated decision-making and profiling The GDPR also covers automated individual decision-making (making a decision solely by automated means) and profiling (automated processing of personal data).

