

## GDPR Fact Sheet

The EU's General Data Protection Regulation (GDPR) replaced the Data Protection Act on 25 May 2018. The rules will still apply even when the UK leaves the EU. GDPR is a complete update and overhaul of existing data protection legislation which dates back to 1995.

The new rules for businesses look at

- The data they **collect**
- The way they **use** the data
- How they **store** the data
- How they **share** the data

Companies who do not comply may be faced with huge fines - up to 20 million euros or 4% a company's global turnover.

Data protection law applies to all personal data about individuals collected or processed in Europe regardless of those individuals' nationality or citizenship. It applies whether the data is on paper or stored electronically.

GDPR applies to all businesses whether they are large or small in every sector and industry.

### Individual Rights

Under European data protection law, individuals retain certain rights over a company's possession and use of the data they hold about them. These rights existing under the previous EU standard but have been greatly enhanced under GDPR. These rights include

1.	The right to be <b>informed</b> about what they are doing with data, specifically through privacy notices
2.	The right of users to <b>access</b> their data
3.	The right to <b>rectification</b> (simply means the right for individuals to correct any incorrect data that a business is holding)
4.	The right to <b>erasure</b> (also known as the "right to be forgotten" meaning people have the right to have certain types of data deleted under certain circumstances)
5.	The right to <b>restrict processing</b> which means the user can ask a business to stop using their data in certain ways
6.	The right to <b>data portability</b> which means the user's right to download the data company's hold about them and upload to a different service provider
7.	The right to <b>object</b> , meaning an individual's right to object to a company's use of their data
8.	Rights in relation to <b>automated decision making</b> and <b>profiling</b> which relates to data used for the purposes of marketing, advertising and behavioural analysis

## The Consent Process

Companies must make sure there are systems in place to collect and process data which are clear, documented and verifiable. The consent process must be

<b>1.</b>	<b>Active</b>	Consent is freely given, specific and unambiguous
<b>2.</b>	<b>Positive</b>	Companies cannot presume consent from a pre-ticked box, inactivity or not selecting any option
<b>3.</b>	<b>Granular</b>	Privacy must be presented as granular multiple. GDPR does not permit “all or nothing”. For example, a customer can object to a business sharing their data with third parties for advertising. It cannot require their data to be shared as a prerequisite for being a customer
<b>4.</b>	<b>Unbundled</b>	Users cannot be forced to grant consent for one thing in order to receive another
<b>5.</b>	<b>Named</b>	The user must be made aware of all specific third parties who will be receiving their data and why they will be receiving it
<b>6.</b>	<b>No imbalance in the relationship</b>	Consent must not create an unfair relationship between the user and the data processor
<b>7.</b>	<b>Verifiable and documented</b>	Companies must be able to prove how consent was given, what information they were given, what they agreed to, when they consented, and whether or not the user has withdrawn consent

Source for this Fact Sheet; <https://www.bgateway.com/documents/guides/GDPR.pdf>

### Links to Short Videos (2 minutes or less)

knox.is/gdpr1: [youtube.com/watch?v=ZfGrp9rhWew](https://www.youtube.com/watch?v=ZfGrp9rhWew)

knox.is/gdpr2: [youtube.com/watch?v=LxltQGoTTfo](https://www.youtube.com/watch?v=LxltQGoTTfo)

knox.is/gdpr3: [youtube.com/watch?v=VLxlogGqCk0](https://www.youtube.com/watch?v=VLxlogGqCk0)