

GDPR Glossary of Terms



GDPR jargon confusing you? We've put together a glossary covering some of the terms of GDPR

Lawful basis of data processing is the need to have a valid lawful reason to process personal data. This could be consent, a legitimate interest or contractual necessity.

Consent is what you request from an individual to access their personal data. It must be freely and willingly given, explicit and require a positive action to opt in. To get explicit consent, you need a clear and specific statement from a data subject that agrees to you processing their data.

Legitimate interest is a valid alternative to consent as a lawful basis for processing—but not for special categories of data. It will not be valid if it harms the rights, interests or freedoms of the individual. You should explain and record your legitimate interest in your GDPR file.

Contractual necessity is the need to process data for an employment contract. It might apply to client agreements and candidate agreements where you have them.

Data subject is a natural person who is the subject of personal data. The data subject is the individual whose personal data is processed by a data controller or data processor.

Personal data is information that relates to a natural person or data subject, which can identify them directly or indirectly. For example a name, ID number, IP address or health information.

Personal data breach is the breach of security that leads to:

- Access of personal data.
- Unlawful destruction of personal data.
- Loss of personal data.
- Change of personal data.
- Unauthorised disclosure of personal data.

A breach can happen to any company that's transmitted, stored or otherwise processed data.

Data controller is a person who (either alone, jointly or alongside other people) makes decisions about how to process the personal data they collect and what to do with it.

Data processor is a natural or legal person (excluding the data controller's employees) who processes data on behalf of the data controller.

Data protection officer (DPO) is a person a company will appoint to be their data expert. They are responsible for making sure a company is GDPR compliant.

Data processing is when a company gets, records or holds information or data. It can also refer to the carrying out of an operation or set of operations on the information or data. This includes data access, storage, retrieval, disclosure and deletion (also called erasure).

Profiling is the automated processing of personal data that a company uses to analyse and predict the behaviour of data subjects.

Right to be informed is the right a data subject has to know how a company will process their personal data. Any information a company gives to the data subject must be concise, clear, understandable and easily accessible. It should also be written in clear, plain language and be free of charge.

Right to access (Subject access right) gives a data subject the right to have complete access to the personal data that a data controller has about them.

Right to be forgotten (Data erasure) gives a data subject the right to have a data controller delete all their personal data.

Right to rectification gives a data subject the right to ask a company to change their personal data if it's inaccurate or incomplete.

Right to restrict processing gives a data subject the right to suppress or block a company from processing their personal data.

Right to object data gives a data subject the right to object to the processing of their information. They can object to:

- Processing based on authentic interests or the performance of a task in the public interest/use of official authority.
- Direct marketing.
- Processing for purposes of research and statistics.

If you have any questions about GDPR, call our brilliant BrightAdvice team today on **0844 892 3928**.