The General Data Protection Regulation (GDPR)

Business Information Factsheet

BIF536 · March 2024

Introduction

The GDPR was originally introduced into the UK as part of European law. However, it was retained in force as the UK GDPR when the UK left the European Union. It requires organisations to comply with data protection principles that give individuals greater control over their personal data.

This factsheet explains what is considered to be 'personal data' under the GDPR and what is meant by 'processing' data. It explains the six lawful bases for processing personal data and the data protection principles that organisations must comply with.

The factsheet is a starting point only. Professional advice should always be taken where necessary.

What is personal data?

'Personal data' means any information relating to an identified or 'identifiable' person. Even where the information held by an organisation does not include the names of individuals, it is still considered to be personal data if it is possible to use the information to work out the identity of the individual it relates to.

Examples of the types of information that might make it possible to identify an individual include:

- Date of birth.
- Postal address.
- IP address.
- A computer cookie.
- Any 'anonymised' identifier that can be traced back to an individual, such as an account code or an online username.

Lawful bases for processing personal data

'Processing' personal data refers to any operation that can be carried out on the data, such as collecting, recording, organising, storing, altering, accessing, using, sharing or destroying it.

Under the GDPR, organisations can only process personal data if they have one or more of six 'lawful bases' for doing so.

The six lawful bases for processing personal data are:

- **Consent:** Where an individual has explicitly agreed to an organisation's request to process their personal data for a specific purpose, the organisation has a lawful basis to process the data for that purpose.
- **Contract:** Where an organisation has a contract with an individual (including unwritten verbal contracts), they have a lawful basis to process that individual's personal data to the extent that is necessary for the performance of the contract.
- **Legal obligation:** This applies to processing that an organisation is legally required to carry out, for example keeping employee records for statutory purposes such as taxation, right to work checks and criminal record checks.
- **Legitimate interests:** If an organisation or a third party has a 'legitimate interest' that makes the processing of an individual's personal data necessary, there may be a lawful basis for processing it. This is the most flexible lawful basis, and legitimate interests can, in principle, cover a wide range of data-processing activities relating to (for example) fraud prevention, IT security and certain types of marketing.
- **Vital interests:** This applies where the processing is necessary to protect someone's life, for example, disclosing an individual's medical records to hospital staff during a medical emergency.
- **Public task:** This usually applies only to public authorities, but it can also apply to other organisations if they are exercising official authority or carrying out a specific task in the public interest that is laid down by law.

Consent

Because consent is only one of six lawful bases for processing personal data, it is not always required. It is more likely to be necessary for organisations that are processing sensitive personal data, such as religious or political beliefs, ethnicity, sexual orientation and medical information.

Where consent is required, organisations must follow strict rules designed to ensure that they seek it in a way that gives individuals genuine choice and control over the types of processing that they agree to.

An individual's indication of consent must involve a positive action (an opt-in). The GDPR prohibits pre-ticked opt-in boxes. When seeking consent, organisations must provide clear information about the data processing that they intend to carry out. If they process data for more than one purpose, they must explain and obtain consent for each purpose separately.

Data protection principles

Under the GDPR, organisations that process personal data must comply with the following data protection principles:

- Ensuring that their handling and use of personal data is transparent, fair and lawful.
- Limiting the processing of personal data to the purposes that they have stated.
- Ensuring that personal data is adequate, relevant and limited to what is necessary for the purposes for which it is processed.
- Ensuring that personal data is kept accurate and up to date.
- Retaining personal data only for as long as is necessary for the purposes for which it was originally collected.
- Ensuring the security of personal data.
- Keeping appropriate records that enable them to demonstrate that they comply with the principles listed above.

Individuals' rights

The GDPR gives individuals several rights in relation to their personal data, including:

- The right to be informed about data relating to them and to access that data.
- The right to have inaccurate or incomplete data corrected.
- The right to have data erased in certain circumstances.
- The right to withdraw consent for their data to be processed.

Complying with the GDPR

The GDPR does not set out a list of specific data protection measures that must always be put in place. Instead, it requires organisations to take measures that are "risk-based and proportionate". For example, an organisation that processes large amounts of sensitive personal data requires a more extensive data protection framework than a smaller organisation that processes minimal personal data.

Examples of data protection measures include the following:

- Having a written data protection policy.
- Displaying a privacy notice clearly explaining the data processing the organisation carries out.
- Regularly reviewing and updating data security measures (such as protection against cyberattacks and malicious software).

- Carrying out a data protection impact assessment before beginning any new data-processing activity.
- Ensuring that data-processing activities, reviews and decisions are fully documented.

Personal data breaches

A personal data breach means any breach of security that leads to personal data being lost, destroyed, corrupted or disclosed. All personal data breaches must be recorded, including the details of the breach, its effects and the actions the organisation has taken in response to the incident.

Serious breaches must be reported to the Information Commissioner's Office (ICO) within 72 hours. For more information, and to report a breach, go to https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-breaches-a-guide.

Useful resources

'UK GDPR Guidance and Resources'
Information Commissioner's Office (ICO)
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources

'Advice for Small Organisations'
ICO
https://ico.org.uk/for-organisations/advice-for-small-organisations

Related factsheets

BIF003 The Data Protection Act 2018
BIF410 A Guide to the Privacy and Electronic Communications Regulations (PECR)

Cobweb Information Ltd, YBN, 7 & 8 Delta Bank Road, Metro Riverside Park, Gateshead, NE11 9DJ.
Tel: 0191 461 8000 Website: www.cobwebinfo.com