An Introduction to Data Protection Law

BHBIA ETHICS & COMPLIANCE | Quick Guide

What is data protection law

Data protection law controls how data or information that could identify an individual is used by an organisation; it protects the rights of data subjects (individuals whom the data is about).

What data protection law applies in the UK

Even though the UK formally left the European Union (EU) on 31 December 2020, the EU's General Data Protection Regulation (GDPR) continues to apply in the UK as it has been incorporated into UK law. The 'UK GDPR' sits alongside an amended version of the Data Protection Act (DPA) 2018.

The data protection requirements that applied in the UK prior to exiting the EU remain largely the same and are largely aligned with those that apply in the European Union, though the UK does have the right to keep the requirements under review.

When UK data protection law applies and who it applies to

The GDPR/DPA 2018 applies to any individual or organisation processing the personal data of UK citizens (based within or outside the UK) for commercial purposes.

The definition of data 'processing' is very broad – it includes the collection, recording, organisation, alteration, retrieval, use, disclosure, dissemination, alignment, combination, blocking, erasure or destruction, or even just storage of personal data.

Anything you do with personal data in the context of providing professional services, from accessing to collecting to using and deleting, is likely to be data processing. It does not apply to processing carried out in a private capacity (for personal/household activities).

Key principles

The key principles that underpin data protection law should guide everything that you do:

- Be transparent about what you do with personal data – with data subjects, within your own organisation, with regulators and the general public
- Be accountable – be able to show that you are compliant by having data protection policies, processes and training in place, and ensuring you and your organisation apply them in practice
- Build privacy in from the start of all your data processing by actively thinking about data protection principles from the very setup of your activities – don't collect more personal data than you need (data minimisation), use anonymisation, pseudonymisation and encryption

Key definitions

Personal data:

- Any information relating to an identifiable living person which does or could identify them.
- May be a single piece or a series of pieces of data which together could allow identification, e.g. a name, email, address, telephone number, but also information that when combined, e.g. a job title and place of work (such as a 'Head of Department' at a specific hospital).
- Can exist in many forms - alphabetic, numeric, photographic, acoustic.

Updated May 2025
Keeping you informed about changes in the UK legal ethical environment.

An Introduction to Data Protection Law

BHBIA ETHICS & COMPLIANCE | Quick Guide

Special category (sensitive) **personal data**:

- Data specially protected under the law referring to race/ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental **health**, sex life and offences plus genetic and biometric data. Additionally, special rules also apply to processing of criminal offence data.
- Special category is sensitive data, e.g. an individual's medical history, and so it has to be treated with extra care which means that we need higher standards of permission to use it and higher standards of security to protect it.

Once all personal data is removed, obscured, aggregated or altered beyond recognition from a data record, the data becomes either anonymised or pseudonymised:

- **Anonymised** – personal data is removed and the data cannot be re-identified; anonymised data is no longer classed as personal data, so it is excluded from GDPR/DPA 2018 requirements.
- **Pseudonymised** – personal data is removed and replaced with a unique code (letters/numbers). As this could potentially be used to re-identify the individual, pseudonymised data is still classified as personal data in the eyes of the law and so must be treated as such.

Data processing roles and agreements

Organisations that process personal data can have different roles relating to their responsibility towards that data:

- **Data Controller** – the organisation responsible for determining the data processing purpose (why) and means (how). It is possible to have two Data Controllers that are jointly responsible for the purpose and means.
- **Data Processor** – an organisation that processes the personal data on behalf of the Data Controller according to the Controller's instructions.
- **Sub-Processor** – an organisation that processes personal data on behalf of the Data Processor.

An organisation's data processing role depends on the specific setup of the project and could change from project to project. It is important for each organisation involved in a MR project to be clear about their data processing role as this determines their legal responsibilities.

Under the UK GDPR/DPA 2018, organisations involved in a MR project must have a **data processing agreement** in place that details their responsibilities and describes the types of data processing and the types of personal data in scope. Usually this is part of the project or services contract. Similar obligations are derived from the EU GDPR.

International transfers of personal data across borders, e.g. to a Data Controller or Data Processor outside of the UK, require additional safeguards for that personal data. This may include additional agreements or clauses if the transfer is to a country without UK 'adequacy regulations' in place.

Lawful bases for data processing

To process personal data organisations must have identified a **'lawful basis'** that allows them to do so, i.e. a reason that holds up in the eyes of the law. There are six possible lawful bases overall that could apply; in MR we generally rely on two of them:

- **Consent** – frequently used in MR –informed consent for the processing of their personal data is given by the individual before that processing begins.

An Introduction to Data Protection Law

BHBIA ETHICS & COMPLIANCE | Quick Guide

- **Legitimate interest** - occasionally used in MR - able to process personal data on the basis that it is necessary to the reasonable (and legal) interests of the organisation. Using this lawful basis is subject to a balancing assessment to determine whether the organisation's interests in the data processing are proportionate to the processing risks to the individual(s) the personal data is about.

Data subject rights and privacy information

The individuals whose personal data is being processed (the 'data subjects') have rights that organisations must respect. Among these are:

- The **right to be informed** – organisations must provide individuals with privacy information (such as in a privacy notice) including: the purposes for processing their personal data, the retention periods for that personal data, and who it will be shared with. This must be shared with individuals at the time their personal data is collected.
- The **right of access** of their personal data – this means data subjects can raise a Subject Access Request to access and receive a copy of their personal data, and other supplementary information.

Useful resources and places to find out more

From the BHBIA

Checklist to help you Audit your Data Processing
Risk and Privacy Impact Assessment
Data Protection Officer
Legal Grounds for Data Processing
Consents for Market Research - what is required and when
Data Security, Breaches and International Transfers

www.bhbia.org.uk/guidelines-and-legislation/privacy-data

From the Information Commissioner's Office (ICO)

UK GDPR guidance and resources
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/

From the Market Research Society (MRS)

Data protection webpage and resources
https://www.mrs.org.uk/standards/data-protection

Disclaimer

This guidance is provided by the BHBIA for information purposes only and is not intended and should not be construed as regulatory or legal advice. It does not cover all legislative and regulatory requirements pertaining to Members and it is the responsibility of all Members to familiarise themselves with these.

British Healthcare Business Intelligence Association
St James House, Vicar Lane, Sheffield, S1 2EX
t: 01727 896085 • admin@bhbia.org.uk • www.bhbia.org.uk
A Private Limited Company Registered in England and Wales No: 9244455

Updated May 2025
Keeping you informed about changes in the UK legal ethical environment.