BHBIA Ethics & Compliance Quick Guide

An Introduction to Data Protection Law

What data protection law applies in the UK

Data protection requirements changed significantly in 2018 when the **General Data Protection Regulation (GDPR)** came into force across the European Union EU). The GDPR is incorporated into UK law through the **UK Data Protection Act (DPA) 2018**. So irrespective of the position or stage of the UK's exit from the EU, GDPR requirements apply and will continue to apply in the UK.

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

When it applies and who to

The GDPR/DPA 2018 applies to any individual or organisation **processing** the personal data of EU citizens (based within or outside the EU) 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, even just storing personal data is data processing.

Anything you do with personal data is likely to be data processing.

Key principles

There are key principles that underpin data protection law, these should guide everything that you do:

- Be transparent about what you do with personal data
- Be accountable – be able to show that you are being compliant by having data protection policies, processes and training in place and using them
- Build privacy in from the start of all your data processing and make it your default option – don't collect more personal data than you need, 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, address, telephone number or when combined a job title and place of work.
- Can exist in many forms - alphabetic, numeric, photographic, acoustic.

Issued August 2020

Keeping you informed about changes in the legal and ethical environment

An Introduction to Data Protection Law

Key definitions continued

Special category/sensitive personal data:

- Data referring to race/ethnic origin, political opinions, religious beliefs, trade union membership, **health,** sex life and offences plus genetic and biometric data.
- Special category is sensitive data e.g. an individual's medical details, 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) but 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, agreements and lawful bases

Organisations that process personal data can have different roles, there is the:

- **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 role they play within 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.

Organisation involved in a MR project must have a **data processing agreement** in place (usually this is part of the contract) that details their responsibilities.

To process personal data organisations must have a '**lawful basis**' i.e. a reason that holds up in the eyes of the law. There are just six possible lawful bases and in MR we generally rely on two of them:

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

Quick Guide
BHBIA Ethics & Compliance

An Introduction to Data Protection Law

BHBIA

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 including Breaches and International Transfers

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

From the Information Commissioner's Office (ICO)

ICO Guide to the General Data Protection Regulation (GDPR)
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

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
Ground Floor, 4 Victoria Square, St. Albans, Herts AL1 3TF
t: 01727 896085 • admin@bhbia.org.uk • www.bhbia.org.uk
A Private Limited Company Registered in England and Wales No: 9244455

Issued August 2020
Keeping you informed about changes in the legal and ethical environment