BHBIA Ethics & Compliance Quick Guide

GDPR

What is GDPR?

GDPR (**General Data Protection Regulation**) is the new legal framework in the EU that replaces the current EU Data Protection Directive. There are many similarities to the UK Data Protection Act 1998, but it also includes new requirements that you need to be aware of.

GDPR came into force on 24th May 2016, but does not take effect until **May 2018**, regardless of Brexit, giving organisations sufficient time to prepare for compliance.

Who does it apply to?

Anyone who is **collecting, storing and processing** the personal data of EU residents i.e. **data controllers** and **data processors**.

What is going to change?

Key changes the GDPR introduces include:

- **An expanded definition of personal data** – it will be much broader, anything that contributes or links to identifying an individual will be included. The definition of sensitive personal data has been expanded to include biometric and genetic data.
- **Greater liability** – for both Data Controllers and Data Processors but particularly for Processors, they can now be held accountable and action taken against them. Controllers will also have the right to audit Processors. Higher fines for non-compliance can be levied – up to 4% of global turnover or €20 million/£15 million.
- **Risk based accountability** – the requirement to notify the ICO of data processing has been removed but risk based accountability now takes an important role. This will impact amongst other things, contracts, privacy notice obligations, risk assessment, record keeping.
- **New and strengthened individual rights** – these include rights of access, to be forgotten, to data portability. Organisations also have an obligation to promote these rights to individuals.
- **Extra-territorial effect** – GDPR requirements will apply if you process the personal data of EU citizens regardless of which country you are based in.

What should you do next?

- Ensure **senior management** are aware of GDPR and the likely impact on your organisation
- Check your **current data status** – what personal data do you already hold, where did it come from and who have you shared it with?
- Review your current **privacy notices** - what updates are needed
- Check your current procedures to ensure you are able to deliver on **all data subjects' rights**. The right to:
    - Be forgotten; have data deleted; a copy of their personal data (within a month, free of charge)
    - Right to data portability – data electronically in a commonly used format
    - Right to prevent automated decisions and profiling

Issued November 2016
Keeping you informed about changes in the legal and ethical environment

BHBIA Ethics & Compliance Quick Guide

GDPR

- Assess how you are **seeking, obtaining and recording consent** – are your records accurate, up to date and secure? Do you have distinct, explicit consent for processing health data?
- Ensure you have appropriate procedures in place to **detect, report and investigate a data breach**.
- Familiarise yourself with DPIAs (**Data Protection Impact Assessments**) and work out when and how to implement these in your organisation (note: exemptions exist for small businesses and small-scale data usage).
- Appoint/ contract a DPO (**Data Protection Officer**) who will be responsible for data protection compliance, acting independently and reporting to the highest levels of management.
- Embed **privacy by design and default** into all projects – don't collect more personal data than you need, use anonymisation, pseudonymisation and encryption
- Make sure your **contracts for all partners** in the market research project chain contain the new provisions.

Useful resources and places to find out more

From the Information Commissioner's Office (ICO)

ICO Overview of the General Data Protection Regulation (GDPR)
https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/
Preparing for the GDPR 12 Steps to Take Now
https://ico.org.uk/media/for-organisations/documents/1624219/preparing-for-the-gdpr-12-steps.pdf

From the Market Research Society (MRS)

Top Ten Tips for GDPR
http://www.fairdata.org.uk/GDPR_top_tips/
Five questions to ask when starting a GDPR Compliance Project
http://www.fairdata.org.uk/GDPR_questions/
GDPR Timeline Guidance Notes
http://www.fairdata.org.uk/GDPR_page

From the BHBIA GDPR Briefing on 8th September 2016

https://www.bhbia.org.uk/archive/eventarchive/newdataprotectionrulesseminar2016.aspx

Disclaimer

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 November 2016
Keeping you informed about changes in the legal and ethical environment