GDPR – How does it affect Research Data Management and data sharing?

GDPR replaces the UK Data Protection Act 1998 and is concerned with the handling of personal data.

It strengthens the rights for data subjects, requires those gathering data to be clear about why and how personal data is to be gathered stored and used, and to document consent given by those they collect data from.

If your research data contains this kind of information, it must be collected and managed in a way that complies with GDPR.

Personal data

Personal data means any information relating to an identifiable person who can be directly or indirectly identified.

"This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people."

(ICO Key Definitions)

Some types of personal data are considered to be particularly sensitive, defined as 'special categories of personal data'. These include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data subjects' rights

Under GDPR, data subjects have the following rights, some of which are new:

- The right to be informed
- The right of access
- The right of rectification
- The right to erasure (to be forgotten)
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

(ICO Individual rights)

Consent

GDPR requires that consent for data collection and use must be freely given, specific, informed and an unambiguous indication of their participants' agreement to the processing of personal data relating to them.

- It must be in the form of a statement or by a clear affirmative action, and cannot, for example, be in the form of a pre-ticked box.
- Consent needs documented so that it can be demonstrated/proved at any point.

To be able to give consent, participants must be informed about, and allowed to give or withhold consent for, each of the ways that their data will be processed and used. Information sheets and consent forms should cover:

- the purpose of the research
- What data will be gathered
- Benefits and risks of taking part
- How data will be stored during the project
- Who will have access to it
- Will it be anonymised or pseudonymised? How and when will this be done?
- Plans for data preservation and sharing
- Contact details for the researcher, institution and funder.

It should also be made clear that they have the right to withdraw their participation from the study and how this can be done.

Participants have the right to erasure (to have their data removed) but it must be stated if there is a point after which this cannot be done (e.g. after anonymization).

The Open University and UK Data Service guidance and templates for writing information sheets and consent forms have been updated for GDPR:

OU sample participant information sheets and consent forms

UK Data Service Guidance and Model consent form

Working with children

When working with children, particular attention should be given to making sure that all information presented to them is age-appropriately understandable and that they are aware of any risks involved.

GDPR allows children aged 16 years or over to give consent for participation. The proposed UK Data Protection Bill lowers may lower this age in the UK, however this is yet to be approved. For children under this age, consent must be sought from whoever holds parental responsibility. A reasonable effort should be made to verify the age of children before taking part, and to verify the responsibility of the adult when asking from consent from them.

(ICO Children)

Data preservation and sharing

Long term preservation and sharing of data is an aim for many and a requirement of many funders, publishers and institutions. To enable this, researchers should detail to participants what data will be preserved and shared, and how open or controlled access will be. For example: "anonymised data will be added to an accessible data repository and openly shared, and non-anonymised data will be stored in an access controlled area or destroyed after a certain period". If access is to be given to non-anonymised data, who will be given access and how?

Anonymised data.

Truly anonymised data – where identifying information is permanently removed and individuals can no longer be identified, and where there is no way to re-identify - is not considered personal data and therefore does not fall under GDPR. However, it may not always be possible to fully anonymise data. As the experts, researchers should decide how effective anonymisation techniques will be for their data. Participants should be informed of the way their data will be anonymised so that they can make an informed decision about consent for its storage and sharing.

Pseudonymised data

Pseudonymisation removes identifying data but retains a way to re-identify, for example where a code in the pseudonymised set can be referenced to identifying information in a separate document. Pseudonymised data is still considered personal data so should be seen as a step towards protecting participants' personal data, but not as a way to make data exempt from the coverage of GDPR.

Transfer outside of the EU

Data can be transferred to countries outside of the EU where the ICO has decided that the receiving country or institution ensures an adequate level of protection, or where the organisation receiving the personal data has provided adequate safeguards. A basis for this type of transfer should be established before transfer is made.

(ICO International Transfers)

Data Management Plans

As always when preparing for data gathering, writing a Data Management Plan will help to foresee and address any issues at the outset.

Questions you should be prepared to answer

- What information will I provide and how will I request consent?
- How will I document consent and how/where will I store it?
- Am I collecting only the personal data that I need?
- Will I anonymise or pseudonymise? How will I do it?
- What if participants request their data? How will I provide it in an accessible way?
- What if participants withdraw? How will I remove their data, and after what point would this become impossible?
- How will I preserve the data long-term?
- Do I plan to share it, and how?

Summary

This guide is not a comprehensive account of every implication and consideration of GDPR on research data, but a pointer to the most relevant areas. A recommended approach is to consider whether your research data falls within the remit of GDPR and what steps you need to take to meet its requirements, referring to guidance from documentation and the relevant support teams at the OU.

In short, you must:

- Inform participants about what you are doing and why you are doing it: explain what information will be gathered, whether and how any identifying information will be removed, and how the data will managed and used during and after the project.
- Request consent for taking part and use of the data at a granular level, allowing participants to consent, or not, to each use.
- Retain documentation of consent
- Store, manage and archive your data in a way that protects personal data

Resources

- The GDPR in full: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG
- GDPR Portal: https://www.eugdpr.org/
- Information Commissioner's Office (ICO) guidance: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr

OU contacts and guidance

- GDPR guidance http://intranet6.open.ac.uk/governance/data-protection/gdpr
- Human Research Ethics Committee (HREC) http://www.open.ac.uk/research/ethics/human-research
- Data Protection http://intranet6.open.ac.uk/governance/data-protection/ou-data-protection-procedures
- Information Security http://intranet6.open.ac.uk/it/main/information-security
- Library Research Support http://www.open.ac.uk/library-research-support/research-data-management

Dan Crane, Library Research Support team

May 2018

- *(updated 04/05/2018)*
- *(updated 22/05/2018 – added information about stating any limits to ability to be forgotten in 'Consent' section)*
- *(updated 29/05/2018 – added link to OU info sheet and consent form*