The EU General Data Protection Regulation (GDPR): Guidance for Researchers

The Act becomes law on May 25th 2018 and governs the processing or using of personal data. Under the law data processing must be **lawful**, **fair** and **transparent.** To ensure fairness, research participants' rights must be protected. This involves ensuring that any data they provide is used in line with the information they have been given about a particular study. In this way transparency about how their data is used is linked to meeting the fairness criterion.

Under the Act researchers may either be
1. **a data controller:** "determines the purposes and means of processing personal data."

or

2. a data processor: "responsible for processing personal data on behalf of a controller."
An important distinction as processors are legally liable if data breaches occur and are required to maintain records of detailing how personal data is processed.

Researchers are likely to fulfill both data controller and data processor roles at different stages of a research process. For example, a funder poses a research question/topic area and provides a budget for the study and a university research team is contracted to address the question. The funder is asking the research team to process data on the funder's behalf. The university team however, decides on what to collect, how to do it, how to analyse and how to present the data. This makes the University team Data Controllers in their own right even although the funder retains overall control of the data as they commissioned it and can determine how they ultimately use the final data report.
This may not always be the case in contract research and role clarification may be necessary. Advice is available from the Data Protection Officer.

The Act applies to:
1. Personal data is defined by the Information Commissioner's Office (ICO) as, "any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier." Identifiers may name, identification number, location data or online identifier, etc.

2. Special categories of personal data" under Article 9**.** As it is sensitive personal data extra protective safeguards have to be in place. The ICO specifies the following as special category data under the Act:

Race	Ethnic origin
Politics	Religion
Trade union membership	Genetics
Biometrics (where used for ID purposes)	Health
Sexual orientation	Sex life

NB "Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing (see Article 10)."

Requirements for Research under the Act

1. Researchers must specify what their lawful basis is for data processing.
University statement that can be used: The University undertakes research as part of its function for the community under its legal status. Data Protection laws allow us to use personal data for research with appropriate safeguards in place under the legal basis of **public tasks that are in the public interest.**

2. For **special categories of data** as defined above, an additional legal basis is required and this is normally that such data processing is **'*necessary for scientific or historical research for archiving in the public interest in accordance with safeguards'*.**

3. Processing **Data Related to Criminal Offences** for research still requires specification of a lawful basis for processing under Article 6, but also needs to comply with Article 10 which says:
"*Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.*"
Further guidance on Data Related to Criminal Offences is to be issued at some point.

Safeguards applied to research in the University context include conformity with the University IT Policies and Procedures to ensure security of all data collected, the University Research Ethics Policies and Procedures, University Research Ethics Committee approval for specific studies, data minimisation, (i.e. only collecting personal data that is essential for a study) and anonymising or pseudonymising (see below) such data whenever possible. There are 10 conditions specified for processing special category data in the Act and these can be found at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/
The ones most relevant to research are:
(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. This is the one most likely to be used.

a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
Consent as part of ethics but consent is not the legal basis for University research.

(e) processing relates to personal data which are manifestly made public by the data subject;

3. The Act talks about **pseudonymised data.** For research, this refers for example to anonymised qualitative data from interviews/focus groups or anonymised quantitative data in longitudinal/ experimental studies where the dataset and the key to identifying the research participants are held within the University. For this reason the data is described as being pseudonymised rather than truly anonymised. Further guidance on psuedonymisation is available from the ICO 'Anonymisation code of practice'

Demonstrating Transparency
The Act requires more emphasis be put on informing research participants about how the data they provide for research is handled. The information that is provided to research participants must be easy to understand and as concise as possible. Information that is provided via web links should also be available in print format for participants who may not have easy web access (leaflets and posters). The recommendation is for a hierarchical approach to dissemination within organisations and the University has adopted this with:
1. **University level Information** delivered via a website with Privacy Statements including one for specifically for research https://www.shu.ac.uk/about-this-website/privacy-policy/privacy-notices/privacy-notice-for-research

This can also be made available as a poster and/or personalised for local Research Institute/ Centre or Department.

2. **Research Centre/ Department Information**:
   a. A privacy statement on the website (Can be personalised but must be approved by Data Protection Officer and Head of Research Ethics).
   b. Posters in waiting areas, laboratories and interview rooms, etc., used by research participants.

3. **Study Specific Information**

Participant information sheets or equivalent statements with the contents required under the Act (see Appendix 1) and consent forms. Under the Act researchers must ensure that the language used in such documents are plain English and where necessary designed to suit the age/cognitive capacity of the research participants.

Participants Rights to Withdraw Data

The Act specifies that existing good ethical practices should be maintained so this means in studies where data is not collected anonymously, participants will still have the right to withdraw their data up until the time specified in the Information Sheet (usually two weeks).

Some of the data rights specified under the Act do not apply to the withdrawal of research data if safeguards as specified earlier are in place. These are:
i) The right of the research participant to access the data they have provided
ii) The right to rectify such data
iii) The right to restrict processing
iv) The right to object to processing.

These limitations to rights only apply where application would "prevent or seriously impair the aims of the research."

The Data Controller (typically the research sponsor) is responsible for making such a claim.
If a research participant wishes to exercise their wider rights under GDPR, the advice of the University Information Officer at DPO@shu.ac.uk must be sought.

International Research

There are specific requirements to meet if personal data is to be transferred to non-EU countries. Advice must be sought from the Data Protection Officer and further guidance will be produced.

Penalties for Non-compliance with GDPR

The ICO have a range of options depending on the severity of the breach
   1) Up to €10 million, or 2% annual global turnover – whichever is higher.
   2) Up to €20 million, or 4% annual global turnover – whichever is higher.

Further Information

SHU Governance Services
>https://portal.shu.ac.uk/sites/GovernanceServices/SitePages/General%20Data%20Protection%20Regulation%20(GDPR).aspx
https://www.shu.ac.uk/about-this-website/privacy-policy/privacy-notices/privacy-notice-for-research

Ann Macaskill & Helen Williamson, 18th May 2018