Research under the General Data Protection Regulation

Background and audience

The General Data Protection Regulation (GDPR) along with the Data Protection Act 2018 (DPA) sets out how personal data and privacy should be managed. The legislation applies to any research project which processes personal information.[1] This also applies to research outside the UK that the University is involved in. Undertaking research in an ethical, fair and lawful manner complies with the requirements for data protection legislation and must start prior to project approval by incorporating data protection and privacy into the research planning process. This guidance is intended to assist researchers with this.

Participant Information Sheet

To comply with fairness and transparency, you will need to provide a Participant Information Sheet ('the PIS' – which for non-research data collection is called the 'privacy notice') for any research project which needs to include the following:

- Who is the data controller (the organisation with the overall responsibility - this will be the University represented by the lead researcher)
- Enough information, in lay language, for the participant to understand what the project is about and what is required of them
- Any significant risks to the participants involved
- Safeguards put in place to limit risks
- Consent to participate in the research
- What the legal basis is that you rely on to make the research lawful (see below "Legal bases for conducting research using personal data"
- Who participants can contact for more information (lead researcher's contact details), a complaints contact and the contact details of this organisation's Data Protection Officer (dpo@ed.ac.uk)
- Details of how people can exercise their rights (see below "Research Participants Rights")
- Assurances that their data will be held securely

[1] 'Personal data' means any information relating to an identified or identifiable natural person ('data subject')

- For special categories of personal data2, compliance with the common law duty of confidentiality
- A note that if the research project changes in any way, the amended PIS will be shown on the project's, Research Centre's, Institute's or School's website.

Depending on your study and if you have a study website, some of the information in the PIS can be placed on the study website. If a website is not suitable, then all information needs to be in the PIS.

The University has published the generic part of the PIS on a website. When you recruit participants, all you need to do is use the appropriate choice of the templates in the appendices to this guidance and link from that document to the generic PIS on the website: https://www.ed.ac.uk/records-management/privacy-notice-research. If you provide the notice in print format you should use the short url: edin.ac/privacy-research.

Templates for PIS are in Appendices B and C.

If the purpose for which you have collected the data changes – if you decide to do follow-on research, or the research plan changes in any way, you will have to inform participants. If at all possible, you will need to issue a new information sheet pointing out the changes. If, however, that is not possible, then there will need to be another way to disseminate the information. Possibilities are posting the new information on the project's website, or, if no such website exists, on the website of the Research Centre, Institute, or School, or making use of social media. This does not apply if the data has been irrevocably anonymised.

Consent

Informed, voluntary and fair consent to participate in a study is the cornerstone of ethical research involving people. It is intended to ensure the rights of individual participants are respected and is closely linked with the participant information sheet. It is through this ethics consent process that research participants can understand what taking part in a specific study will mean for them, so they can make an informed choice to either take part or decline.

To summarise, you will need ethics consent to participate such as "I agree to participate in the ... study." linked to the participant information sheet. Note, however, that you will **not** need to obtain consent for processing, sharing or storing the research date. An example of this consent form can be found in Appendix A.

[2] Special categories of personal data are physical and mental health data, data relating to race or ethnicity, to political opinions or religious beliefs, trade union membership, criminal convictions, sexual orientation, genetic data and biometric data.

Legal bases for conducting research using personal data

Personal data

In most circumstances the legal basis for using personal data for research will be 'public task'. This is evidenced in the generic part of the PIS with a statement making reference to the University's public research purpose as established by the Universities (Scotland) Act 1966. By using 'public task' as the legal basis, we can ensure that as a publicly-funded organisation, it is always one of our official, public tasks when we use personal data from people who have agreed to take part in research, and that you are part of a reputable organisation that has a genuine reason to hold and use personal data. This is in addition to the control given to participants through the research ethics consent (to participate in research) process.

Special categories of personal data

If the research contains health data including genetic and biometric data, information about race or ethnicity or religious/philosophical beliefs, then you will need to have an additional legal basis for processing the data. In addition to the reference to the research being a public task as stated in the generic PIS, the legal basis will be 'processing ... necessary for … scientific or historical research purposes in accordance with Article 89(1)'. This leads to the requirement for so-called safeguards in Article 89(1) for all research processing special categories of personal data and you will need to ensure that you comply.

Article 89(1) safeguards

The new legislation has been written with research in mind, and most of the safeguards needed will already be familiar to you and are likely to be present in most scientific research already. These safeguards consist of technical and organisational measures and provide research participants with assurance that their personal data is:

- Necessary to support research,
- Will only be used to support legitimate research activities that are considered to be in the public interest,
- Their interests are safeguarded/protected, and
- Not be likely to cause substantial damage or distress to an individual.

Technical and organisational measures are:

- The minimisation principle – use only the absolute minimum of personal data required for your purpose
- Anonymise personal data if you can
- If you cannot anonymise, wherever possible, pseudonymise all personal data
- Store the data securely

Besides having these technical and organisational measures in place, you must be able to prove that you research is in the public interest. Similar to the technical and

organisational measures, the types of evidence for proving that research is in the public interest will be familiar to research and very likely already in place.

Public interest test – examples of evidence:

- Your research must be proportionate
- Your research is subject to a governance framework
- Research ethics committee (REC) review (does not have to be a European REC)
- Peer review from a funder

Confidentiality Advisory Group (CAG) recommendation for support in England and Wales or support by the Public Benefit and Privacy Panel (PBPP) for Health and Social Care in Scotland

Specifics for using medical or other confidential data

For some kinds of medical research, you must still comply with other relevant statutes and requirements such as the Human Tissue Act.

Please also note that the common law duty of confidence will not be affected by the implementation of the GDPR and DPA. While personal data and confidential information will frequently overlap, they are not identical. Information is considered confidential under common law if:

- It is not in the public domain, and It can be related to an identifiable individual who can be living or deceased, and
- It has a degree of sensitivity associated with it, and
- It is given with the expectation that it will be kept confidential, such as due to the relationship between a patient and their doctor, nurse, researcher, etc.

Research initiated before 25 May 2018

If a study has started before 25 May 2018, i.e. before the new data protection legislation came into force, you do not have to do anything as you can rely on the consent that you have originally obtained from the research participants. If the study started before 25 May 2018 and is still recruiting, the same consent form can still be used. If you want to conduct any follow-on studies, you will not have to re-consent the participants, instead, you can rely on the legal basis of ‘public task’.

Research Participants’ Rights

You can restrict the rights of research participants if you believe that granting them would prevent or seriously impair the achievement of the research purpose, however, only where ‘appropriate safeguards’ are in place. The lead researcher will make the final decision.

In these circumstances, you can restrict the following rights:

- The right to rectification
- The right to restrict processing

- The right to object to processing
- The right to erasure (right to be forgotten)

To evaluate whether granting these rights would prevent or impair research, you will need to consider timing: The decision is always context dependent and may change during the course of a study. For example, the request to erasure by a single individual from a research project may be easier to facilitate and therefore would have little impact on the study. The same request from ¾ of the participants of that project would have a serious impact on the study. At the same time, the possibility of the participants in, for example, a clinical trial suffering distress is exponentially greater than participants in a paper-based survey.

At a reasonably early stage of a study it could be possible to meet a research participant's request for erasure without significantly impairing the quality or validity of research in a way that might not be possible at a later stage.

Take into consideration:

- resource implications
- available technology

In addition, you will not have to comply with subject access requests, where:

- the results of the research or any resulting statistics will not be published in an identifiable form, or
- in the opinion of an appropriate health professional, disclosure to the data subject is likely to cause serious harm.

You should seek the advice of your local Data Protection Champion first before responding to any exercise of a data subject's rights.

Find your local Data Protection Champion

You can also ask the University's Data Protection Officer for advice, who can be reached at dpo@ed.ac.uk**.**

Data Protection Impact Assessments (DPIA)

A DPIA is an assessment to help you identify any potential risks a project might have as regards intruding into participants' privacy. The DPIA then assists with implementing appropriate measures and controls to minimise and manage those risks. The legislation has made DPIAs mandatory to ensure that privacy and data protection are key considerations from the start of any project and then taken into account throughout the project's lifecycle.

For most studies, the DPIA is included in the internal Research Ethics Committee approval process, however, some funders will require a separate DPIA. If this is the

case, seek the advice of your local Data Protection Champion who will be able to direct you to the template and guidance.

You can also ask the University's Data Protection Officer for advice, who can be reached at dpo@ed.ac.uk**.**

About this guidance

Version control	Author/editor	Date	Edits made
2	Data Protection Officer	26 June 2018	Initial version for web created by DICM.

If you require the guidance in an alternative format, please contact Records Management: recordsmanagement@ed.ac.uk or 0131 651 4099