GDPR and Research – An Overview for Researchers

What is GDPR?

The EU General Data Protection Regulation (GDPR) and the UK Data Protection Act 2018 govern the processing (acquiring, holding, using, etc.) of personal data in the UK.

Although the new legislation has not been designed specifically for research, it is important that you, as researchers understand what GDPR means for you and the personal data that's processed during your research.

The Information Commissioner's Office (ICO) is the regulator and provides guidance for compliance with the new legislation in their GDPR guide, which applies to all types of sectors and is not research-specific.

Organisations that process personal data, or control its processing, are accountable for compliance with the new legislation through their Data Protection Officers and research management functions. In the case of academic researchers, these organisations will be your universities. For researchers in Independent Research Organisations (IROs), these will be the organisations to seek advice from. Data Protection Officers and research management teams are a good, local source of advice for you.

What counts as 'personal data'?

Personal data is data that relates to living people from which they can be directly or indirectly identified - direct identifiability being from the data itself, or indirect identifiability being from the combination of the data with other available data. The ICO provide detailed guidance on this – for more information see What is personal data?

Data that has been pseudonymised (with identifiers separated) may still be personal data, depending on how hard it is to reconnect the identifiers with the dataset. Robust controls that separate the two - for example, a legal agreement that prevents reidentification and controls access to the identification key - will help protect the data so that it may be possible to classify it as not personal data to those that do not have access to the key.

It is also worth noting that the action of anonymising counts as processing personal data for the purposes of GDPR.

At the time of writing, the ICO is working to develop new guidelines on anonymisation, which will be published in due course. The advice given by the UK Anonymisation Framework is also useful in this regard.

How does GDPR impact research?

GDPR was not designed to impede research and allows research certain privileges. It recognises that any data can be useful for research, and that research can be a long-term endeavour – for example, the ICO say data can be stored for research indefinitely, where the controller has set out legitimate justification for such indefinite retention. Research can therefore be exempt from the purpose and storage limitations as long as the other data protection principles and specific safeguards are met.

The new law demands that data processing is **lawful**, **fair** and **transparent.** UKRI-funded research organisations will have an obvious lawful basis for their research activity (see below). The greatest changes are around implementing new transparency requirements and meeting the necessary safeguards, where these do not already reflect current good research practice. In health and social research, for example, the safeguard requirements can largely be demonstrated by reference to existing university research governance systems (e.g. assurance that ethical approval is in place).

How do I make sure my data processing for research is lawful?

All research organisations must meet all legal requirements relevant to the processing activity (e.g. common law of confidentiality) and specify a lawful basis for data processing for their activities. If you are processing personal data for research purposes, you should know the lawful basis you are relying on because you may be asked to specify it. There are six lawful bases and at least one must apply.

The most likely lawful basis for research in UKRI Institutes and in universities (as public authorities) is '*task in the public interest*'. Organisations can demonstrate they meet the requirements to use this lawful basis by reference to their legal constitutions, or because they are operating under a relevant statute that specifies research as one of the purposes of the organisation, e.g. for universities: University Charter, Education Reform Act, Universities Scotland Act; for UKRI research institutes: Higher Education and Research Act. Using this lawful basis helps to assure research participants that the organisation is credible and using their personal data for public good.

For non-public authorities such as charities and commercial research organisations (e.g. Independent Research Organisations) '*legitimate interests*' is likely to be the appropriate lawful basis for processing personal data for research. This helps to assure participants that there are compelling reasons for processing their personal data for research.

Consent is another lawful basis for processing personal data but researchers need to bear in mind that:

1. The ICO say that you are likely to consider consent when no other lawful basis applies.
2. Consent as one of GDPR's lawful bases for legally processing personal data is different to, and should not be confused with, consent that researchers usually seek from people to participate in a project (see below).

When processing special categories of data, like personal data about health, ethnicity, political opinions, religious beliefs, etc., you must meet an additional condition. In these cases, the most likely condition will be that such processing is '*necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with safeguards'.*

In research, we usually seek consent from people to participate in a project. This is ethical, and needed for other legal reasons, for example if disclosing confidential information or if running a drug trial. Consent discussions should include all relevant aspects of the research project including any sharing of confidential information, so participants can make an informed decision about whether to take part. Therefore, it is important to continue to include the processing of personal data, if that is part of the project, in research consent discussions. However, 'consent', as defined by GDPR, is not likely to be the lawful basis for processing personal data for research purposes; therefore, the consent requirements of GDPR are unlikely to apply to research.

What do I need to do to be fair and transparent?

Being fair with research participants includes respecting their rights and ensuring that personal data is used in line with their expectations. Transparency is therefore intrinsically linked to fairness. The fairness and transparency requirements give control to participants: they have greater awareness of how their data is being used and can object if they wish.

The new legislation sets out the transparency information that should be provided to participants (information does not need to be provided to participants if they already have it). Transparency information must be concise, easy to understand and easy to find.

Transparency information is best provided at both the corporate and research project levels (a layered approach). Work with your Data Protection Officer to ensure that the information you provide to participants is coordinated, relevant and understandable, and explains how data is used to support research. Good research transparency should help participants understand that data is commonly linked with other data sources, kept for a long time, reused to address important research questions

and how their interests are protected, as well as meeting all other transparency requirements as outlined in the link above.

Organisations should display corporate privacy information about research where people will notice it, for example, links on website homepages. Help your participants to notice privacy information using communication methods appropriate for your study population, for example, links from participant information sheets. You can provide further detail in departmental or project materials.

It's important to use best endeavours or appropriate measures to help people notice transparency information. What these measures look like depend on the level of contact you have with participants. Where you have direct contact, e.g. if you interview participants as part of your research, or you regularly communicate with them via a newsletter, there are obvious routes to provide them with information. If you have no direct contact with participants, using other methods that are appropriate for your study population will be needed (e.g. notices in waiting rooms, social media or local newspapers). Discuss the appropriate measures with your Data Protection Officer.

Where data was not collected from participants, but from other sources, there are exemptions to transparency requirements if the provision of information is 'impossible' or involves 'disproportionate effort'. In these circumstances GDPR transparency information must be publicly accessible as a minimum, further efforts to help people notice it are not required. If you think this exemption might apply, discuss this with your Data Protection Officer.

What are the implications for sharing my data?

UKRI supports the principles in the Concordat on open Research Data that recognise that research data should wherever possible be made available for use by others in a manner consistent with relevant legal, ethical and disciplinary frameworks and norms. The GDPR does not prevent research data from being archived and shared for research use by others, as long as the data protection principles are met. An example is where researchers collect data directly from participants, you should discuss their intention to reuse in further research and to deposit in an archive. Where participants expect their data to be kept confidential, sharing can only take place with the participant's permission or through another legal avenue if their permission cannot be obtained (e.g. for confidential patient information s251 support from the Confidentiality Advisory Group in England and Wales; Caldicott Guardian or Public Benefit and Privacy Panel approval in Scotland; or equivalent in Northern Ireland). Sharing all individual participant level data should be through managed processes, with controls over access and usage, in order to protect participants from the risks of re-identification.

What are GDPR safeguards?

Safeguards are protections for participants, and include (but are not limited to):

- not causing substantial damage or distress to research participants (research ethics approval helps here);
- not making decisions or measures that affect individuals on the basis of research personal data (this is not likely to be relevant for the majority of research). There is an exception to this for ethically approved medical research;
- respecting the principle of data minimisation, i.e. processing personal data that's adequate (sufficient to fulfil the research purpose), relevant and limited to what is necessary;
- anonymising or pseudonymising, where possible;
- understanding the importance of privacy, confidentiality and security (working to your employer's codes of conduct, IT policies and technical standards will help here);
- meeting a separate public interest test for processing special categories of personal data over and above using *'task in the public interest'* as the lawful basis, such as peer review from a public funder or research ethics committee approval.

Who's responsible?

Data controllers (i.e. organisations, through their Data Protection Officers) are accountable to the ICO, so you, as a researcher, shouldn't make decisions relating to legal compliance alone. Ensure you know which organisation is the data controller for your research. This might be the organisation you work for, or in health research it will most likely be the sponsor of your project (which is usually the substantive employer of the Chief Investigator). You may even have more than one controller. Talk to your Data Protection Officer, research managers or to your data support services.

This is particularly important if a research participant asks you about their personal data rights, for example if they ask to withdraw from your study. Data Protection Officers are responsible for managing requests about rights and will know how to apply the exemptions that are available to research, which are conditional on meeting further safeguards.

Data Protection Officers also have to meet the new accountability requirements, which you may need to feed into (e.g. Data Protection Impact Assessments).

There are specific requirements for transferring personal data to non-EU countries which may impact international collaborative research. Again, if this applies, seek advice from your Data Protection Officer.