

GDPR: Implications for research

The General Data Protection Regulation (GDPR) applies to any 'personal data' processed by organisations in the EU, and personal data of people in the EU that is processed anywhere.

Personal data is data relating to living people from which they can be identified. This is very broadly defined, and includes data containing names, postcodes, photos, email addresses, bank details, social networking posts, and unique online identifiers including IP addresses, etc. It even includes data that has been pseudonymised (but not data that has been anonymised in line with the [ICO code of practice](#))*, and covers data that is either automatically generated or manually collated.

** Data protection law does not apply to data rendered anonymous in such a way that the data subject is no longer identifiable. There are strict guidelines in place determining whether or not data is truly anonymous.*

Particularly sensitive data - such as data about health, political opinions, religious beliefs, or genetic or biometric data that is uniquely identifying - are classed as special categories of personal data and require additional protection.

How does it affect me as a researcher?

The regulation requires you to be lawful, fair and transparent. Each is equally important.

In order to be lawful, anyone who processes personal data needs to comply with one of six 'legal bases' for doing so. The appropriate one for publicly funded university research is likely to be the fact that processing is necessary to perform a 'task in the public interest'. This assures research participants that the organisation is credible and using their personal data for public good. Commercially funded research is most likely to be carried out under the 'legitimate interest' legal basis.

Where special categories of data are processed, such as health data, an additional condition is needed. This is likely to be 'necessary for scientific research in accordance with safeguards'.

Safeguards apply widely to the processing of personal data for research, not just for special categories. These safeguards should already be in place as part of current good practice. They include obtaining Research Ethics Committee approval, only processing personal data that's necessary (data minimisation), and anonymising or pseudonymising where possible.

Data should be held securely with an appropriate level of protection, and those handling the data should be aware of the importance of confidentiality.

What about consent?

The GDPR has created some confusion around consent. Consent can be understood in two different ways: as one of the six lawful bases under GDPR (this is consent as the lawful basis for processing personal data); and as consent to take part in a research project because of ethical or other legal requirements.

Under GDPR if you are using 'task in the public interest' as the lawful basis plus the research condition for special categories of personal data, you do *not* need to meet the 'consent' requirements of GDPR, such as getting reconsent from participants every two years.

However, just as you do now, you will still need to seek initial consent from participants to take part in your research project. This is for ethical or other legal reasons, such as [disclosing confidential information](#) in line with the common law of confidentiality. Consent to participate in research can give participants control over how their data are used.

So participants have dual assurance: the GDPR ‘task in the public interest’ reassures them that the organisation processes personal data for the public good, and the existing systems by which they consent to participate give them control over how their data is used.

Fair and transparent

As well as being lawful, your research using personal data will need to be fair and transparent.

Fairness includes respecting participants’ rights and ensuring that personal data is used in line with their expectations.

Transparency is very important for fairness. There are [new requirements](#) covering the information that needs to be provided to participants. Transparency will be addressed at the corporate level in privacy notices, but also at project level. The materials you provide are often where participants get their understanding of what will be done with their personal data, so you need to be clear and transparent in the detail you give.

Participants should understand the research process. You need to explain how data is used in research, who will see it, and how long it will be retained for. Explain how their privacy will be protected. If you do this in all materials, participants will understand the value of their data to the research endeavour and have reassurance that their personal interests are being safeguarded.

Institutional Process

The Research Office will ask you to provide details of any personal data processing activities within your research projects, together with details of the legal basis by which you are collecting the data, at the point of application.

This will enable us to evidence our compliance, which is a key requirement of the new regulation.

Further assistance

Further information is available on the University’s dedicated web pages:

<http://www.lboro.ac.uk/admin/ar/policy/dpact/>

<http://www.lboro.ac.uk/services/registry/information-governance/>

Your School’s Data Coordinator and / or Operations Manager will be able to provide additional assistance.

The Research Office can also provide support for queries relating to the use of research data. Please contact your school RDM in the first instance.