



**The British
Psychological Society**
Promoting excellence in psychology

Data Protection Regulation: Guidance for researchers



December 2018

GDPR guidance for researchers

Background

The rules for handling information relating to research participants changed on 25 May 2018, when the new EU General Data Protection Regulation (GDPR) came into force. The Data Protection Act (2018) also became law on 23 May 2018.

The new legislation brings increased expectations of organisations (such as universities, research units and other research organisations) processing personal data. Organisations need to be lawful, fair and transparent when processing or controlling the processing of personal data. However, the new legislation is not intended to impede research. It reflects current good practice in research, through the safeguards that apply to all research using personal data. If your organisation is already following good practice under current data protection legislation, you will need to make relatively few changes to your policies and practices. Your data protection officer should be able to assist you with any queries regarding your research data.

Some aspects of the new legislation do not apply to research. For example, data can be stored for research for long periods of time, and it is recognised that personal data collected for any initial purpose can be used for research. There are also exemptions to some rights in a research context. However, neither rights nor general principles of research ethics can simply be ignored.

So what do researchers need to know?

General principles: The GDPR sets out seven key principles:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

These principles should lie at the heart of your approach to processing personal data.

Legal basis for processing

Organisations must have a valid, legal reason to process personal data (called a 'legal basis'). There are six available lawful bases for processing. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the individual.

Most lawful bases require that processing is 'necessary'. If you can reasonably achieve the same purpose without the processing, you won't have a lawful basis.

You must determine your lawful basis before you begin processing, and you should document it. Take care to get it right first time – you should not swap to a different lawful basis at a later date without good reason.

The six legal bases are:

- Consent
- Contract
- Legal obligation
- Vital interest
- Public interest
- Legitimate interest

For further information on each of these, go to: <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/>

Implications for research

Legal basis for processing

For the majority of research, NHS organisations, universities and Research Council institutes will no longer be able to use 'legitimate interests' as the legal basis for processing. Instead, they should use 'task in the public interest' as their legal basis. Public authorities should document their justification for this, by reference to their public research purpose as established by statute or university charter.

Consent

Under the GDPR, consent is defined as:

'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.'

Consequently, using 'consent' as the legal basis for processing is unlikely to be appropriate for research due to the strict demands of GDPR compliant consent. Other legal bases for processing (such as public interest or legitimate interest) are not subject to such stringent requirements. Nevertheless, gaining research consent is obviously an integral part of the research process and obtaining such consent should be included in any research proposal. Consent for research purposes should not be confused with consent as the legal basis for processing personal data. Researchers are advised to follow the best practice principles set out in the *Code of Human Research Ethics* and the *Guidelines for Conducting Internet Mediated Research*.

For research conducted in a private organisation or charity, 'legitimate interests' will typically be the most appropriate legal basis for processing.

Anonymised/de-identified data

The removal of identifying information from data which prevents an individual from being identified means that the data are no longer considered personal data and therefore do not fall under GDPR.

Pseudonymisation may be appropriate and replaces identifying names in data but retains a way to re-identify (for e.g. using a code within a data set that can be referenced to identifying information in a separate document). This is a useful step towards protecting participants' personal data but is not exempt from the requirements for GDPR. However, it may not always be possible to fully de-identify data even if names are changed.

Participants should be informed about the way in which their data will be anonymised/de-identified so that they can make an informed decision about consent for its storage and sharing.

Legal basis for processing 'special category' personal data

'Special category' personal data are:

- data which reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership;
- data concerning health (the physical or mental health of a person, including the provision of healthcare services);
- data concerning sex life or sexual orientation; or
- genetic or biometric data processed to uniquely identify a natural person.

'Genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.

Whether processed by a public authority or by a commercial organisation or charitable research organisation, special category personal data can be processed for research purposes, but only if processing such data is:

- necessary for archiving purposes, scientific or historical research purposes or statistical purposes;
- subject to appropriate safeguards; and
- in the public interest.

For further guidance: <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/>

Children

Children need particular protection when you are collecting and processing their personal data because they may be less aware of the risks involved.

If you process children's personal data then you should think about the need to protect them from the outset, and design your systems and processes with this in mind.

Compliance with the data protection principles and in particular fairness should be central to all your processing of children's personal data.

You need to have a lawful basis for processing a child's personal data. Consent is one possible lawful basis for processing, but it is not the only option. Sometimes using an alternative basis is more appropriate and provides better protection for the child.

If you are relying on consent as your lawful basis for processing personal data, when offering an online service directly to a child, only children aged 13 or over are able provide their own consent (as set out in the Data Protection Act, 2018).

For children under this age you need to get consent from whoever holds parental responsibility for the child.

Individual rights: Exemption for research

The GDPR provides the following rights for individuals:

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

In some circumstances, the DPA (2018) provides exemptions from particular GDPR provisions when personal data is processed for scientific or historical research purposes or statistical purposes. There are exemptions from the right to access, the right to rectification, the right to restrict processing and the right to object. If the exemption applies, you may not have to comply with all the usual rights and obligations.

There are also exceptions from the right to erasure (for personal data to be deleted); however, this would only apply if complying with the provision would prevent or seriously impair the achievement of the purposes for processing. So, for example, if the deletion of data is requested during or after statistical analysis has been completed and the individual cannot be identified from the research results.

Useful resources

Code of Human Research Ethics

www.bps.org.uk/news-and-policy/bps-code-human-research-ethics-2nd-edition-2014

Guidelines for Conducting Internet Mediated Research

www.bps.org.uk/news-and-policy/ethics-guidelines-internet-mediated-research-2017

Information Commissioners Office

www.ico.org.uk

Health Research Authority

www.hra.nhs.uk/about-us/news-updates/gdpr-guidance-researchers/

ESRC

<https://esrc.ukri.org/funding/guidance-for-applicants/research-ethics/>

Medical Research Council

<https://mrc.ukri.org/research/facilities-and-resources-for-researchers/regulatory-support-centre/gdpr-resources/>

The British Psychological Society

St Andrews House, 48 Princess Road East, Leicester LE1 7DR, UK

Tel: 0116 254 9568 Fax 0116 247 0787 Email: mail@bps.org.uk

Website: www.bps.org.uk

INF316/12.18