General Data Protection Regulation (GDPR) – Information for researchers

Summary

The General Data Protection Regulation (GDPR) will affect the way personal data is processed but the new legislation will not impede research. Continued good practice as established in full compliance with the Data Protection Act 1998 will ensure the majority of data protection requirements are achieved, however, it is important that researchers are aware of the differences between the Data Protection Act and the GDPR.

Under the GDPR there are 7 principles relating to processing of personal data:

1. Lawfulness, fairness and transparency;
2. Purpose limitation;
3. Data minimisation;
4. Accuracy;
5. Storage limitation;
6. Integrity and confidentiality;
7. Accountability.

What is GDPR?

The EU General Data Protection Regulation applies from 25 May 2018. It governs the processing (holding or using) of personal data and is implemented in the UK by the Data Protection Act 2018.

Requirements largely mirror current good practice in research under the Data Protection Act 1998. However, it is important researchers familiarise themselves with the GDPR to ensure appropriate data protection in all their research activities.

What information does the GDPR apply to?

The GDPR applies to ‘personal data’ and ‘special category personal data’ and there are a few differences from the Data Protection Act 1998 to reflect changes in technology.

What counts as ‘personal data’?

‘Personal data’ is data about living people from which they can be identified, either directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

Personal data that has been ‘pseudonymised’ – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

Data that has been anonymised is considered to be out of the scope of the GDPR, although the act of anonymisation constitutes processing of personal data.

What counts as ‘special category personal data’?

The GDPR refers to sensitive personal data as ‘special category personal data’ and additional safeguards are required to process data of this type.
‘Special category personal data’ is defined as: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a person, data concerning health or data concerning a person’s sex life or sexual orientation.

**What counts as ‘processing’?**

‘Processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

**Principles relating to processing of personal data**

Personal data shall be:

<table>
<thead>
<tr>
<th>a) Processed lawfully, fairly and in a transparent manner in relation to the data subject</th>
<th>‘lawfulness, fairness and transparency’</th>
</tr>
</thead>
<tbody>
<tr>
<td>b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered incompatible with the initial purposes</td>
<td>‘purpose limitation’</td>
</tr>
<tr>
<td>c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed</td>
<td>‘data minimisation’</td>
</tr>
<tr>
<td>d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay</td>
<td>‘accuracy’</td>
</tr>
<tr>
<td>e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures in order to safeguard the rights and freedoms of the data subject</td>
<td>‘storage limitation’</td>
</tr>
<tr>
<td>f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures</td>
<td>‘integrity and confidentiality’</td>
</tr>
</tbody>
</table>
How do I make sure my data processing for research is lawful?

While participant consent for collecting personal data for research purposes will still be an ethical requirement, the lawful basis for data processing for research purposes in universities has been agreed as ‘task carried out in the public interest’. Public authorities such as universities, the NHS, research council institutes, receive public funding to conduct tasks that are considered to be in the public interest.

Justification for this lawful basis is set out in the University Charter: ‘the objects of the University are to advance education and disseminate knowledge by teaching, scholarship and research for the public benefit’ (paragraph 3).¹

The University’s Data Protection Officer can advise if the researcher believes their research may need to rely on a different lawful basis to process personal data: https://www.kent.ac.uk/infocompliance/dp/contact.html

Additional safeguards required for processing of special category personal data for research purposes

To process ‘special category personal data’ for research purposes a further condition must be fulfilled in addition to the ‘public task’ lawful basis. For organisations such as universities this is set out in the GDPR as:

Article 9(2)(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 refers to Article 89(1) which outlines safeguards that are likely to be present in most scientific research already. In universities these safeguards include:

- Research Ethics Committee review and approval
- Governance checks (including Health Research Authority assessment for health research)
- Peer review from public funders
- Data minimisation and minimisation of recruitment numbers
- Pseudonymisation and other technical safeguards against accidental disclosure and loss or corruption of research data.

These governance arrangements 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, and
- Their interests are safeguarded/protected.

¹ See: https://www.kent.ac.uk/governance/documents/about/charterdocs/2010-10-04_Kent_Charter.pdf (viewed 08.05.18)
These organisational assurances are in addition to the controls research participants have on the use of their personal data through the normal research consent process.

Researchers must ensure their research complies with these established University governance procedures in order to legitimise the use of special category personal data for research purposes.

**Consent in research**

Historically, most research studies that have involved use of confidential information have sought consent from participants. This meets ethical expectations to promote the autonomy and privacy of research participants. Legally, consent is obtained to avoid a breach of the common law duty of confidentiality, especially relating to health information. This is not changing with the introduction of the GDPR.

The GDPR sets out the expectation that consent would not be appropriate as a lawful basis for processing personal data for research purposes, where there is an imbalance of power in the relationship between the controller and the data subject, e.g. where the controller is a public authority and the data subject depends on their services, or fears adverse consequences, so feels they have no choice but to agree. Furthermore, consent should not be used as the lawful basis under the GDPR if the subject’s rights that follow from consent under the legislation (e.g. right to withdraw) cannot be applied, for example because it would limit the validity of the research.

The consent process is a mechanism to ensure the rights of individual participants are respected, and to enable participants to understand what taking part in a study will mean for them, so they can make an informed choice on whether to agree to take part.

The consent process also helps researchers to fulfil the first GDPR Principle to be fair and transparent in how they hold and use personal data by providing participants with information about how they intend to use it, and the types of data they will be using, etc.

- **‘Opt-out’ consent**
  Under GDPR, where consent is to be relied on as the lawful basis for processing personal data, it must be explicit, and so ‘opt-out’ consent would not be compliant.

  However, because the lawful basis for the majority of University research is expected to be ‘task carried out in the public interest’, and consent will be sought for ethical reasons, opt-out consent would still be acceptable with the appropriate ethical clearance.

  The University has previously advised that for research involving children, vulnerable participants or sensitive personal data, opt-out consent would not be considered appropriate.

**Data subject rights**

The GDPR incorporates a range of data subject rights, but because the new legislation was written with research in mind, exemptions mean that these may be limited in the context of research to avoid compromising data validity.
The following data subject rights may be limited:
- The right to erasure
- The right to access by the data subject
- The right to rectification
- The right to restrict processing
- The right to object to processing.

However, where consent is relied on as the lawful basis for processing personal data (rather than ‘task in the public interest’ as would be usual for University research) these rights will still apply.

The following data subject right is not applicable to research under public interest (university research):
- The right to data portability.

Where a participant seeks to use one of the above rights advice should be sought from the University's Data Protection Officer.

While consent procedures should allow participants to withdraw from the project should they wish, it is important to make clear during consent procedures any limits to this right, e.g. until the point that any data collected has been anonymised and/or aggregated.

---

**As a researcher, what do I need to do?**

Firstly, continue good practice in processing research data as established under the Data Protection Act 1998.

Secondly, follow the points below to ensure compliance with the GDPR.

**Privacy notices**

One of the ways to ensure transparency in personal data processing in compliance with the first GDPR Principle is to draw up a privacy notice. The GDPR makes explicit what has always been set out as good practice. For research this has historically been fulfilled by providing information to participants as part of the consent process. To ensure optimum transparency it is recommended that this information is provided to participants under the heading: ‘**How your information will be used**’. The information provided to research participants about how their personal data will be processed as part of a research project must be:

- concise, transparent, intelligible and easily accessible
- written in clear and plain language, particularly if addressed to a child
- free of charge.

The notice must include the following information:

- What information is being collected?
- Who is collecting it?
- How is it collected?
- Why is it being collected?
- How will it be used?
• Who will it be shared with?
• What will be the effect of this on the individuals concerned?

Getting the privacy notice right could reduce the number of queries from individuals and boost participation in research.

In addition to the project-specific privacy notice that must be included in participant information, it might be appropriate to provide departmental or research group level information. A University-level privacy notice that contains corporate level information that will be the same for all University research has been published on the University website and a link to this can be included in participant information.


Safeguards

Safeguards are the measures taken to ensure the data is processed securely, accurately and in accordance with data protection principles.

The GDPR places strong emphasis on implementing safeguards for processing personal data for research. This means consideration must be given to the arrangements for security and storage of data, including pseudonymisation or anonymisation of data wherever possible. Personal data should only be collected when needed (data minimisation) – if some or all of the research activities can be undertaken without using identifiable personal data then arrangements should be made to do so. Obtaining a favourable opinion from a research ethics committee provides further safeguards.

Data Protection Impact Assessments – DPIAs

Individual DPIAs will not be required for the majority of research projects carried out by staff and students. Data protection measures in research projects are already assessed as part of the research ethics review procedure. Research ethics review is a requirement for all University research involving human participants (Research Integrity: Code of Ethical Practice in Research – https://research.kent.ac.uk/researchservices/wp-content/uploads/sites/51/2017/04/Research-Integrity-Code-of-Ethical-Practice-in-Research.pdf ). Template research ethics review documentation has been updated in compliance with GDPR requirements.

However, DPIAs are mandatory for high risk processing of personal data for research projects involving:

• **Sensitive data or data of a highly personal nature:** this includes special categories of personal data as defined in Article 9 as well as personal data relating to criminal convictions or offences as defined in Article 10.

• **Data concerning vulnerable data subjects:** the processing of this type of data is a criterion because of the increased power imbalance between the data subjects and the data controller, meaning the individuals may be unable to easily consent to, or oppose, the processing of their data, or exercise their rights. Vulnerable data subjects may include children, employees, more vulnerable segments of the population requiring special protection (mentally ill persons, asylum seekers, or the elderly, patients, etc.) and in any case where an imbalance in the relationship between the position of the data subject and the controller can be identified.
- **Systematic monitoring**: processing used to observe, monitor or control data subjects, including data collected through networks or “a systematic monitoring of a publicly accessible area” (Article 35(3)(c)). This type of monitoring is a criterion because the personal data may be collected in circumstances where data subjects may not be aware of who is collecting their data and how they will be used. Additionally it may be impossible for individuals to avoid being subject to such processing in public (or publicly accessible) space(s).

- **Data processed on a large scale**: while not explicitly defined in the GDPR the following factors should be considered when determining whether the processing is carried out on a large scale:
  - The number of data subjects concerned, either as a specific number or as a proportion of the relevant population;
  - The volume of data and/or the range of different data items being processed;
  - The duration, or permanence, of the data processing activity;
  - The geographical extent of the processing activity.

- **Matching or combining datasets**: for example originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject.

For research projects involving any of the above elements advice on whether a DPIA is required should be sought from the Data Protection Officer: [https://www.kent.ac.uk/infocompliance/dp/contact.html](https://www.kent.ac.uk/infocompliance/dp/contact.html)

### Data breaches

Data breaches must be notified to the University’s Data Protection Officer immediately at [https://www.kent.ac.uk/infocompliance/dp/contact.html](https://www.kent.ac.uk/infocompliance/dp/contact.html) The University is required to notify the Information Commissioner’s Office of data breaches within 72 hours and so there must be no delay. The GDPR has introduced significant fines for data breaches.

Researchers will need to notify affected data subjects if the breach will cause significant risks to their individual rights.

It is important researchers have mechanisms in place to ensure that data breaches are noticed and recognised as a breach. Data breaches can include:

- Unauthorised access by a third party
- Deliberate or accidental action/inaction by a controller/processor
- Sending personal data to the wrong person
- Devices containing personal data being lost or stolen
- Alteration of personal data without permission
- Loss of availability of personal data.

A data breach can occur at any time and not always within office hours. Where it is not immediately possible to notify the Data Protection Officer damage limitation action should take priority. This can include:

- Taking down a webpage
- Informing unauthorised recipients of an email to delete it and not to share it
- Informing IT Services if an account has been hacked.
More information on data breaches, the notification procedure and damage limitation is available on the Information Compliance webpages here:

https://www.kent.ac.uk/infocompliance/dp/staff-info/data-breach.html

References


Medical Research Council Regulatory Centre GDPR – What researchers need to know: https://www.insight.mrc.ac.uk/2018/04/16/gdpr-research-changes/

JISC GDPR resources: https://www.jisc.ac.uk/gdpr

University of Kent – Information Compliance: https://www.kent.ac.uk/infocompliance/dp/staff-info/staff-info.html


Nicole Palmer
Research Ethics & Governance Officer
May 2018