The General Data Protection Regulation (GDPR): Research and Archiving FAQs

UK Data Service
Author:      Dr Scott Summers, UK Data Service  
Updated:     July 2018  
Version:     2  

Suggested citation  
Contents

1. What is the GDPR? 4
2. What is ‘personal data’? 4
3. What is meant by ‘special categories data’? 5
4. What is meant by ‘pseudonymisation’ and ‘anonymisation’? 5
5. What is the difference between a ‘data controller’ and a ‘data processor’? 6
6. Who will be the data controller for personal data collected in a research project? 6
7. Where does the GDPR apply? 6
8. Who will be the supervisory authority for the GDPR in the UK? 6
9. What are the principles that need to be complied with when processing personal data? 7
10. What are the bases for processing personal data? 7
11. What are the additional conditions needed for processing special categories of personal data? 8
12. What are the requirements for gaining informed consent? 8
13. What does informed consent mean for research? 8
14. What does informed consent mean for archiving and data sharing? 9
15. What does informed consent mean when gaining consent from children? 9
16. Does the GDPR permit the archiving of research data? 10
17. What are a data subject’s rights under the GDPR? 10
18. What information should be provided to a data subject when personal data are collected from them? 10
19. Can data be transferred outside of the EU? 11
20. Where can I find the full text of the legislation? 12
This document seeks to answer many of the frequently asked questions which researchers may have about the General Data Protection Regulation (GDPR). This document focuses its discussion around research and archiving research data. This is based on the best knowledge and advice available at the time of writing (July 2018). As this is a fluid area of law where updated guidance and advice is being published by the Information Commissioner’s Office (ICO) and the Article 29 Working Party on a regular basis, we cannot fully guarantee the accuracy of the information contained within this document. **This document does not constitute, and should not be construed as, legal advice.** We will publish updated versions of this document as more guidance comes to light in the coming months.

1. What is the GDPR?

The GDPR is the new EU-wide data protection regulation that came into force on the 25 May 2018, replacing the then UK Data Protection Act 1998 (DPA). The GDPR enables data subjects to have greater control over their personal data, whilst also modernising and unifying European data protection rules. As well as creating new rights for data subjects, the GDPR also strengthens and enhances previous rights that data subjects held under the DPA. The GDPR requires data controllers and processors to provide clarity, transparency and accountability to data subjects about how and why their personal data is being processed.

The GDPR permits EU Member States – in certain areas – to make specific domestic provisions (e.g. derogations) for particular aspects of the GDPR. The UK Government has achieved this through the Data Protection Act 2018, which should be read alongside the GDPR.

2. What is ‘personal data’?

The GDPR defines ‘personal data’ as ‘any information relating to an identified or identifiable natural person’ (‘data subject’). An identifiable natural person is defined as one ‘who can be identified, directly or indirectly, 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 natural person.’

---

1 Council Regulation 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.
2 Data subjects are those who are the subject of that specific personal data.
5 The GDPR Article 4(1).
6 ibid.
The GDPR applies only to the data of living persons.\(^7\) Data which do not count as personal data do not fall within the scope of data protection legislation; however, there may still be ethical reasons for wishing to protect this information.

3. What is meant by ‘special categories data’?

Certain ‘personal data’ are considered to be particularly sensitive and have therefore been given specific protection within the GDPR;\(^8\) these include:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data;
- Biometric data;
- Data concerning health;
- Data concerning a natural person’s sex life or sexual orientation.

Those familiar with the provisions of the existing DPA will recognise that many of these data were already classified as ‘sensitive personal data’ under UK data protection law.

4. What is meant by ‘pseudonymisation’ and ‘anonymisation’?

The GDPR defines pseudonymisation as the process of making personal data such that they can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person\(^9\). Therefore, pseudonymised data, ‘which could be attributed to a natural person by the use of additional information, should be considered to be information on an identifiable natural person’\(^10\).

Anonymisation – on the other hand – involves processing the personal data in a way to ‘irreversibly prevent identification’\(^11\). Therefore, anonymous data is data that is rendered in such a manner that the data subject is ‘not or no longer identifiable’\(^12\). It is worth noting though, that in practice it can be hard to ‘truly’ anonymise data\(^13\) and this is particularly true for qualitative research data.

---

\(^7\) The GDPR Recital 27.
\(^8\) The GDPR Article 9(1).
\(^9\) The GDPR Article 4(5).
\(^10\) The GDPR Recital 26.
\(^12\) The GDPR (n 10).
\(^13\) Article 29 Working Party (n 11), p5.
5. What is the difference between a ‘data controller’ and a ‘data processor’?

A ‘data controller’ is the person or organisation which, alone or jointly with others, determines the purposes and means of the processing of personal data.14 Whereas a ‘data processor’ is the person or organisation which processes personal data on behalf of the data controller.15

It should be noted that a data processor can also now be liable under the GDPR for damage it has caused to a data subject in certain circumstances, such as, where the processing has infringed the GDPR or where the processor has acted outside the lawful instructions of the data controller.16

6. Who will be the data controller for personal data collected in a research project?

This is a decision that the institution will need to make. However, in most cases it will unlikely be the individual researcher, and more likely the University that the researcher works for who is the data controller. If the researcher were to be designated as the data controller, then they must ensure they register themselves as a data controller with the supervisory authority in the UK (See FAQ 8).

7. Where does the GDPR apply?

The GDPR applies to any data controller or data processor in the EU who collects personal data about a data subject of any country, anywhere in the world.17 This means that a researcher based within the EU who collects personal data about a participant, from any other country within the world, needs to comply with the GDPR. A data controller or data processor that is based outside the EU but collects personal data on EU citizens will also be covered by the GDPR.

8. Who will be the supervisory authority for the GDPR in the UK?

In the UK, the supervisory authority – who will enforce the GDPR – will be the Information Commissioner’s Office (ICO).

---

14 The GDPR Article 4(7).
15 The GDPR Article 4(8).
16 The GDPR Article 82(2).
17 The GDPR Article 3(1).
9. What are the principles that need to be complied with when processing personal data?

The GDPR specifies six principles that need to be adhered to when processing personal data.\textsuperscript{18}

1. **Process lawfully, fairly and transparently.** In practice, this should mean that the data subject is informed of what will be done with the data and the data processing should be undertaken accordingly.

2. **Kept to the original purpose.** Data should be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

3. **Minimise data size.** Personal data that are collected should be adequate, relevant and limited to what is necessary.

4. **Uphold accuracy.** Personal data should be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay.

5. **Remove data which are not used.** Personal data should be 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.

6. **Ensure data integrity and confidentiality.** Personal data should be 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.

10. What are the bases for processing personal data?

There are six bases for the processing of personal data, and one of these must be present in order to process a data subject’s personal data.\textsuperscript{19}

1. Consent of the data subject;
2. Necessary for the performance of a contract;
3. Legal obligation placed upon controller;
4. Necessary to protect the vital interests of the data subject;
5. Carried out in the public interest or is in the exercise of official authority;
6. Legitimate interest pursued by controller.

In the context of research, there appears to likely be three most applicable grounds for the processing of personal data: (i) consent or (ii) public interest (public task) or (iii) legitimate interest. It will be essential that an assessment is made by the data controller for each individual research project to identify the most appropriate grounds for the processing of the personal data for that project.

---

\textsuperscript{18} The GDPR Article 5.

\textsuperscript{19} The GDPR Article 6.
It is also important to note that the processing ground does not have to be consent, it can be another. Researchers should still gain informed consent for their other ethical and legal obligations, but use a different ground – where it is more appropriate – for the processing of the personal data.

Where consent is used as the processing ground for personal data it should be ‘distinguished from other consent requirements that serve as an ethical standard or procedural obligation’.20

11. What are the additional conditions needed for processing special categories of personal data?

When processing special categories of personal data an additional condition from Article 9 of the GDPR is needed. This condition, along with the Article 6 lawful basis for processing the personal data, must be documented by the data controller, and conveyed to research participants in a transparent manner.

Scientific research is specifically mentioned in Article 9 (2)(j) of the GDPR: Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1).

12. What are the requirements for gaining informed consent?

The GDPR specifies that consent needs to be freely given, informed, unambiguous, specific and by a clear affirmative action that signifies agreement to the processing of the personal data.21 This will mean, for example, that pre-ticked boxes will not be an acceptable form of gaining consent in the future.

When special categories data are processed – and the processing basis for this is consent – there is a further requirement to the above that this must be based on explicit consent.22

Under the GDPR, consent needs to be documented, which means (in the context of research) it will be important for researchers to maintain documented and accurate records of the consent obtained from their participants. This could, for example, be written consent or audio recorded oral consent. Though the GDPR does not require this consent to be in a written form, many UK research ethics committees and professional bodies do require this or recommend it as best practice.

13. What does informed consent mean for research?

To obtain informed consent when conducting research, researchers should:

- Inform participants about the purpose of the research;
- Discuss what will happen to their contribution (including the future archiving and sharing of their data);
- Indicate the steps that will be taken to safeguard their anonymity and confidentiality; and

---

21 The GDPR Article 4(11).
22 The GDPR Article 9(2)(a).
• Outline their right to withdraw from the research.

When seeking to obtain informed consent from participants, it is important for researchers to also consider the specific circumstances and needs of the participants. This may mean, for example: pictures or diagrams are used on the consent form instead of using a lot of text or the consent form is translated into another language.

The GDPR recognises that it is often not possible to fully identify the purpose of the personal data processing in research at the time of data collection and, therefore, data subjects should be able to give their consent to certain areas of the research (in keeping with recognised ethical standards for research).

14. What does informed consent mean for archiving and data sharing?

Gaining informed consent for archiving and data sharing should be seen as ‘one more small step’ to gaining informed consent from participants to participate in a research project. By adding the discussion of data sharing and archiving to the consent process, it permits the participant to make an informed decision. This empowers them by allowing them to choose whether they wish for their contribution to the research project – and their data – to be available for use in future research projects.

The best way to achieve informed consent for archiving and data sharing is to offer the participant the option to consent (on a granular level) to what will be included in the archiving process and to seek to identify and explain the possible future uses of their data.

How might this look in practice? In a qualitative study, this could be achieved by allowing the participant to decide which parts of their input to the study can be archived for future reuse, such as: the anonymised transcripts, the non-anonymised audio recordings and the non-anonymised photographs.

15. What does informed consent mean when gaining consent from children?

The GDPR permits children over the age of 16 to be able to provide consent to data processing. Where a child is under the age of 16, consent can be sought from the holder of parental responsibility over the child. However, under the Data Protection Act 2018, the UK has provided that children over the age of 13 will be legally able to provide consent.

As highlighted above in the ‘What does informed consent mean for research?’ section, when gaining consent from children, it is imperative that researchers consider the specific needs of the child participant and how best to ensure they fully understand and can engage effectively in the consent process.

---

23 The GDPR Recital 33.
24 The GDPR Article 8, note this is in specific relation to ‘information society services’.
25 The Data Protection Act 2018 Article 9.
16. Does the GDPR permit the archiving of research data?

Absolutely. The GDPR makes express provisions for both research and archiving.\(^{26}\) However, both are subject to appropriate safeguards for the rights and freedoms of data subjects. These safeguards require that technical and organisational measures are in place in order to ensure respect for the principle of data minimisation.

In practice, this means Principles two and five – which must be complied with when processing personal data (see FAQ 9) – are less strict. Further processing of research data for the purposes of archiving, scientific or historical research purposes and statistical purposes is not considered to be incompatible with the initial purposes (even when this purpose was not expressly mentioned earlier). Personal data may also be stored for longer periods for such purposes.

17. What are a data subject’s rights under the GDPR?

Data subjects derive a number of rights under the GDPR; some of these are new rights and others are rights that they already hold under the DPA:

- The right to be informed;
- The right of access;
- The right of rectification;
- The right to erasure (the ‘right to be forgotten’);
- The right to restrict processing;
- The right to data portability;
- The right to object;
- Rights in relation to automated individual decision-making and profiling.

18. What information should be provided to a data subject when personal data are collected from them?

When data are collected from the data subject, the following information should be provided to them:\(^{27}\)

- The identity and contact details of the data controller (and the Data Protection Officer, where applicable);
- The legal basis and purpose of the processing of the data;
- The recipients – or categories of recipients – of the data;
- If applicable, the fact that data will be transferred to a third country or international organisation and the existence or absence of an adequacy decision by the European Commission, reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available;
- The period of retention for holding the data or the criteria used to determine this;
- Information informing the data subject about their rights to access, rectification, erasure, restriction of processing and portability of their data;
- When the processing is based upon consent, the data subject must be informed of their

---

\(^{26}\) The GDPR Article 89.

\(^{27}\) The GDPR Article 13.
right to withdraw their consent (which will not affect the lawfulness of the processing based on consent before withdrawal);
• When the processing is based on the necessity for the performance of a contract, the possible consequences of failure to provide the personal data as part of the contractual requirement;
• A reminder that they have the right to lodge a complaint with the ICO; and,
• If the controller intends to process the personal data for a purpose other than that for which the personal data were collected, the data subject should be informed prior to that further processing with information on the other purpose and with any relevant further information.

19. Can data be transferred outside of the EU?

Personal data may be transferred to a third country where the European Commission has decided that the country has an adequate level of protection. This decision will be based on the European Commission taking account of various factors which can be found under Article 45(2) of the GDPR. When an ‘adequacy decision’ is in place this means that any data transfer to that third country shall not require any specific authorisation.

In the absence of an ‘adequacy decision’ personal data can only be transferred to a third country where the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. The appropriate safeguards may be provided for via one of the following and do not require specific authorisation from the ICO: a legally binding and enforceable instrument between public authorities; binding corporate rules; standard data protection clauses (which have been adopted by the ICO and authorised by the European Commission); an approved code of conduct or approved certification together with binding and enforceable commitments of the controller or processor and appropriate safeguards.

In the absence of either of the above, there are derogations for specific situations in Article 49 which may permit the transfer. This includes the case where the data subject has expressly consented to the purpose of the transfer after having been informed of the possible risks of such a transfer due to the absence of an adequacy decision and appropriate safeguards.

When choosing where to store personal data, it is important to consider how best to protect that data and whether it is appropriate for it to be transferred or stored outside the EU. Personal data should be sought to be minimised, anonymised and / or pseudonymised – where appropriate – and ensure that technical measures such as encryption are utilised to help to protect that data.

---

28 The GDPR Article 45(1).
29 Ibid.
30 The GDPR Article 46(1).
31 The GDPR Article 46(2).
32 Which are in accordance with Article 47 of the GDPR.
33 The GDPR Article 49(1)(a).
20. Where can I find the full text of the legislation?

The GDPR text can be found here,\textsuperscript{34} and the UK Data Protection Act 2018 here.\textsuperscript{35}

