General Data Protection Regulation (GDPR) and research: a guidance note

This note seeks to help prepare researchers to ensure regulatory compliance following the introduction of the UK General Data Protection Regulation (UK GDPR); and to meet best practice in research ethics and governance.

This note is not intended as the final authority on data protection regulations. Researchers should always consult with the UK GDPR, the Data Protection Act 2018, the Information Commissioner's Office guidance, guidance from the regulatory authorities such as the Health Research Authority, and colleagues in Legal and Governance for definitive guidance on data protection practice. This note should be read in conjunction with the resources set out in the 'Determining the lawful basis' section of this document.

Background

At time of writing, the UK's data protection legislation comprises of two main pieces of legislation, the UK General Data Protection Regulation which has been adopted into UK law and amended to fit the UK's needs following Brexit. This legislation is complemented by the Data Protection Act 2018, which provides specific exemptions and schedules specific to UK institutions and needs. Together, the two pieces of legislation set out how UK institutions should manage personal data.

Defining personal data

'Personal data' includes pseudonymised data, and is defined as:

> "… any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, 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 natural person."[1]

Reviewing your practices for the processing of personal data

Researchers should regularly review the steps in place to protect personal data. Elements such as consent processes, transparency information, and your mechanisms for data storage and data use should be subject to ongoing review to ensure that good practice standards are met and that participant's rights and wishes are respected.

Providing information on the lawful basis for processing personal data to research participants

The UK General Data Protection Regulation requires each activity of processing data to have a lawful basis.

For studies falling under the Department of Health framework, the Health Research Authority have produced guidance on the requirements for providing information on the lawful basis to research participants, and this guidance must be followed for studies requiring review by the Health Research Authority.

The University processes personal data as part of its research and teaching activities in accordance with the lawful basis of 'public task', and in accordance with the University's Supplemental Charter which states that the purpose of the University "shall be to advance education, learning and research for the public benefit".

[1] General Data Protection Regulation, Article 4 (a definition of pseudonymised is provided in Article 4)

Further information on fulfilling the requirements for using public task as your lawful basis for processing personal data can be found in the resources section below.

In order to inform research participants about the lawful basis on which you are processing their personal data, you will need to use the University template participant forms.

Participant information sheets and consent forms

In order to ensure compliance with the GDPR principles, researchers should use the latest template participant information sheets provided either by the University for studies approved by a University research ethics committee; or by the Health Regulatory Authority for studies approved by a NHS research ethics committee.

All information provided to participants must be concise, transparent, in easily accessible form, and made using clear and plain language to meet the needs of the audience. Please see the guidance below for information on informed consent.

The University's template participant information sheets and consent forms~~,~~ are available at:

Research ethics webpages - template participant forms

The only exception to the requirement to use the University templates would be where these documents need to be tailored to meet the needs of the research population; for example, child-friendly forms which may include pictures and diagrams.

International transfer of data

The General Data Protection Regulation applies whenever personal data is transferred out of the EU, and the Regulation imposes specific restrictions on the transfer of personal data outside the European Union to third countries or

international organisations. For the purposes of data protection, the UK is classed as "adequate" and is free to transfer data within the EU with no additional obligations.

Personal data may only be transferred outside of the EU in compliance with the conditions for transfer set out in Chapter V of the General Data Protection Regulation.[2]

Where practical and appropriate, the University should have a contract or similar agreement with the party (or parties) regularly receiving the data outside the EU, this contract must include appropriate data protection clauses.

Where the University is transferring personal data outside the EU on an irregular or ad-hoc basis, this is only permitted where the transfer is:

- made with the individual's informed consent
- necessary for important reasons of public interest[3]

When transferring personal data outside the EU, you must ensure that you have informed consent from research participants to cover the transfer. You must also ensure that the arrangements for protecting the confidentiality of the data meet the highest levels of confidentiality and security.

The IT Services Department can provide advice on the security mechanisms that can be used to protect personal data when transferring data outside of the EU.

[2] General Data Protection Regulation, Chapter V

[3] Information Commissioner's Office: International transfers

General good practice in data collection and management

The General Data Protection Regulation offers an opportunity to review and refresh existing practices to ensure that they meet recommended best practice standards and regulatory requirements in the collection and management of personal data collected during research. Please visit the University's research data management webpages for additional guidance.

Informed consent

The definition of consent outlined when using consent as the lawful basis for processing personal data has been refined in the Regulation as: "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".[4] Whilst this represents good practice in obtaining consent for a wide range of activities, is recognised that research studies will not normally be able to meet these requirements, which is why the University uses 'public task' as it's lawful basis for processing personal data. However, it should be emphasised that this does not affect the ethical importance of consent or the common law requirements for consent.

It is important to distinguish between consent for a participant to join a study or consent required under the common law duty of confidentiality from consent to process personal data under the GDPR. It is highly unlikely consent is the best lawful mechanism to use personal data in most instances.

Consent means offering individuals real choice and control. Genuine consent should put individuals in charge, build trust and engagement, and enable participants to decide whether or not to take part in the study.

[4] General Data Protection Regulation, Article 4

The following extract outlines some of the good practice considerations for obtaining informed consent:

- Consent should be a positive opt-in
- Explicit consent requires a very clear and specific statement of consent in words, rather than by any other positive action
- Keep your consent requests separate from other terms and conditions
    - Avoid making consent to processing a precondition of any service you are offering
- Keep evidence of consent – who, when, how, and what you told people.
    - Participant consent forms should be stored securely and confidentially
- The participant information sheet and consent forms should:
    - Outline the lawful basis, ‘public task’, on which the University processes personal data (and the condition for processing if sensitive data is collected)
    - Be specific and granular where possible to get separate consent for separate things
    - Explain why you want the data (purpose), and you will do with it (intended use), and how long the data will be stored
    - Explain who, if anyone, the data will be shared with; and in what format the data will be shared
    - Highlight what you are doing to ensure the security of personal information
    - Be clear, concise, user friendly

- Make it easy for people to withdraw consent to participate in research, and tell them how they can withdraw their participation (explaining any limitations to withdrawing or deleting their data)

- Explain that the participant has the right to complain to the University and the Information Commissioner's Office if they are unhappy with the data management

- Contain the contact details of the Principal Investigator and the University of Liverpool Data Protection Officer

- Keep consent under review, and refresh it if anything changes.

You must keep clear records to demonstrate consent; and these must be stored securely and confidentially.

It should be noted that it may not always be possible to achieve the gold standard criteria for consent as outlined above. Explicit and granular consent is not always compatible with recommended good practice in certain types of research. For example, consent obtained for research using human material samples often lacks 'explicit consent', as to do so could lead to the unnecessary destruction of a unique resource. In such cases, a broader consent is obtained to allow the future use and sharing of personal data under certain conditions which have been reviewed and approved by a research ethics committee.

Research data management

Under the General Data Protection Regulation, there is a greater emphasis on implementing safeguards for personal data. This means that you should give consideration to the arrangements for the security and storage of data; ensure that data are pseudonymised or anonymised wherever possible, and as early as possible; and that personal data are only collected when needed (known as 'data

minimisation'). If you can undertake some or all of your research activities without using identifiable personal data, you must make arrangements to do so.[5]

Primary responsibility for the management of data produced during research activities lies with the Principal Investigator (or Supervisor). Where research is conducted with other institutions and independent researchers, University of Liverpool researchers are responsible for the management of research data held by the University that is under their own control.[6]

The following extract outlines some of the good practice considerations for research data management:

- Wherever possible, data should be anonymised or pseudonymised. Personal data can only be disclosed when explicit and documented permission to disclose is part of the consent procedure.[7]

- Store data on a secure and regularly backed up site - this should be on server systems operated by the University's IT Services Department (University network drive)[8]

    - Storage of data on locations other than the University networked drives should be approved by Information Security colleagues in the Computing Services Department

    - Further information on the correct processes for storing your research data can be found on the Research Data Management webpages

[5] Health Research Authority: Guidance for Researchers

[6] University Research Data Management Policy

[7] University Policy on Research Ethics

[8] University Information Security Policy

- apply technical controls to limit access to the data
    - University network drives and Microsoft SharePoint contain features which enable users to limit access to the data
- use encryption to digitally secure the data
    - Further information on encryption can be found on the IT Services webpages
- ensure that hard copies of any data (that cannot be digitised) are held in a physically secure location
    - For student projects, hard copies of any personal data should be kept in a locked filing cabinet in the Supervisor's office
- provide secure deletion and destruction facilities
    - Colleagues in Records Management and IT Services can advise on retention and disposal of research data
- Sharing personal data should only be done with the consent of research participants
    - A research ethics committee (or in the case of NHS research, the Confidential Advisory Group) should review any proposal to share data without participant consent

The confidentiality of the information supplied by research participants and the anonymity of respondents must be respected.

Sensitive personal data

The Regulation refers to sensitive personal data as “special categories of personal data” in Article 9 of the regulation. Sensitive personal data includes information revealing an individual’s:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;

… or involves the processing of:

- genetic data;
- biometric data for the purpose of uniquely identifying a natural person;
- data concerning health
- data concerning a natural person's sex life
- data concerning a natural person's sexual orientation.[9]

Special category data is personal data which the Regulation says is more sensitive, and so needs more protection as this type of data could create more significant risks to a person’s fundamental rights and freedoms.

[9] General Data Protection Regulation, Article 9

A data protection impact assessment is required for processing that is likely to result in a high risk to individuals – for example, where any special category data is processed. The data security measures should be as rigorous as possible when processing sensitive personal data.

If you are processing special category data, you will need to outline both the lawful basis for processing ('public task') and the separate condition for processing this data. The condition on which the University processes special category data is that the "processing is necessary for archiving purposes in the public interest".

Please refer to the Information Commissioner's Office guidance on special category data for further information on the conditions.

When processing special category or criminal offence data, it must be recognised that the risk to the rights and freedoms of persons are heightened from processing this data; as processing may give rise to discrimination, financial loss, damage to the reputation, loss of confidentiality of personal data, and any other significant economic or social disadvantage. Therefore the likelihood and severity of the risk to the rights and freedoms of the data subject should be carefully considered alongside the nature, scope, context and purposes of the processing to determine whether processing is necessary and whether the safeguards mitigate the risk.

Criminal offence data

Article 10 applies to personal data relating to criminal convictions and offences, or related security measures. Criminal offence data includes the type of data about criminal allegations, proceedings or convictions that would have been sensitive personal data under the 1998 Act; including personal data linked to related security measures.

Processing of personal data relating to criminal convictions and offences can be carried out only under the control of official authority or when the processing is

authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects.[10]

If you are processing criminal offence data, you will need both a lawful basis for processing ('public task') and a separate condition for processing this data under Article 9. This can be met using Article 9 (2) (j) – the condition for scientific and other research. This condition is then further qualified by the additional condition housed at Schedule 1, Section 1, Paragraph 4 of the Data Protection Act 2018.

Please refer to the Information Commissioner's Office guidance on criminal offence data for further information.

Human Material, consent and GDPR

The consent provisions for the collection and storage of human material are unchanged by the implementation of the General Data Protection Regulations (GDPR). Consent remains a requirement of Common Law and the common law duty of confidentiality[11] is not affected by the implementation of GDPR**.** The Human Tissue Authority (HTA) have therefore not provided any changes to the current advice or guidance on this matter (HTA COP A: Guiding Principles and the Fundamental Principle of Consent[12]).

The University's guidance on best practice for consent involving human material can be found by referring to -The University of Liverpool Human Material Code of

[10] General Data Protection Regulation, Article 10

[11] https://www.health-ni.gov.uk/articles/common-law-duty-confidentiality

[12] Human Tissue Authority Codes of Practice

Practice-HTA003[13] and The University of Liverpool supporting document-Consenting for research SDS001[14].

As outlined in earlier sections, the Implementation of GDPR does change the requirements for organisations to hold and process personal data and special categories of personal data.

Consent to participation in research is not the same as consent as the legal basis for processing under data protection legislation. Consent is obtained for participation in research, but the lawful basis which the data collected will be processed under is defined in the study transparency statement.

Guidance produced by the Medical Research Council (MRC) and the Health Research Authority (HRA) state that for public authorities such as Universities, NHS organisations, Research Council institutes or other public authority the lawful basis under which they hold and use personal data is most likely to be GDPR Article 6(1)(e)[6] a **'task in the public interest'**[15][16]

> *GDPR Article 6(1) (e) "Processing is necessary for the **performance of a task carried out in the public interest** or in the exercise of official authority vested the controller;"*

You should note that if it would be possible to undertake your research without processing personal data then your intended legal basis will not be valid.

---

[13] University Human Material Policies and Standard Operating Procedures

[14] See footnote 13

[15] UK Research and Innovation GDPR: Lawful basis, research and confidentiality guidance note

[16] Health Research Authority GDPR guidance - Consent in research

The MRC[5] have also provided guidance on which of the separate conditions from Article 9 would most likely be used by public authorities to hold and use special categories of personal data

GDPR 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"[17].

Further processing of data

When personal data has been collected from a data subject but the controller (either the University or the Sponsor) intends to further process the data for a different purpose, the controller must also give the data subject information about that further purpose before the data is processed. An example is that researchers may wish to use personal data originally collected for clinical or local audit for research.

However, if the information about further processing is in fact the same as the information for the original processing, the data controller does not need to give the data subject that information again[18].

[17] http://www.privacy-regulation.eu/en/article-9-processing-of-special-categories-of-personal-data-GDPR.htm

[18] https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/gdpr-detailed-guidance/transparency/

Reporting requirements

The Regulation introduces a duty on all organisations to report personal data breaches to the relevant supervisory authority. You must do this within 72 hours of becoming aware of the breach, where feasible.

As soon as you become aware of a personal data breach, you must report this to the Director of Legal and Governance, Mr Kevan Ryan (kevan.ryan@liverpool.ac.uk) and the University Data Protection Officer, Mr Dan Howarth (dhowarth@liverpool.ac.uk) who will then advise on the next steps for handling the breach.

Additional notes

Although the theme of the General Data Protection Regulation is around empowering individuals' data rights and reshaping the way organisations approach personal data processing, there are a number of areas where the Regulation does not provide specific and conclusive authority with regard to research.

For example, there are no specific provisions to cover the collection of data obtained from behavioural observation studies, the use of data which is available in the public domain, etc. In such areas where there is no specific legislative provision, the spirit of the Regulation, existing common law, and best practice guidance should be considered when reviewing the processing of the personal data. Relevant considerations should be reflected upon in your research ethics applications.

Determining the lawful basis for processing personal information in research

The General Data Protection Regulation requires each activity of processing data to have a lawful basis. There are around six lawful bases for processing personal data. The Information Commissioner's Office have produced a 'Lawful basis guidance tool' to help determine the most appropriate lawful basis for your processing.

For studies falling under the Department of Health framework, please see the Health Research Authority guidance on the lawful basis for processing.

The University processes personal data as part of its research and teaching activities in accordance with the lawful basis of 'public task', and in accordance with the University's Supplemental Charter which states that the purpose of the University "shall be to advance education, learning and research for the public benefit". Further information on fulfilling the requirements for using public task as your lawful basis for processing personal data can be found below.

Public interest

The Health Research Authority note "For health and social care research, the legal basis is determined by the type of organisation: for universities, NHS organisations or Research Council institutes the processing of personal data for research will be a 'task in the public interest'".[19]

When relying on 'public interest' as the lawful basis for processing, the following points need to be considered:

- Are you processing the data to carry out your official tasks or functions, or other specific tasks in the public interest?
    - The University considers the collection of personal data for the purposes of advancing education, learning and research to be a public task
- Can you point to a clear basis in law for your task or function?

[19] Health Research Authority: GDPR Operational Guidance

- The University considers the advancement of education, learning and research to be the basis in law for the collection of personal data in research

- Is there another reasonable way to perform your tasks or functions without processing the data?

  - The processing must be necessary. If you could reasonably perform your tasks or exercise your powers in a less intrusive way, this lawful basis does not apply.

You need to be sure that you can demonstrate why processing is necessary to perform a task in the public interest and that there is no other reasonable way to perform the task without processing personal data. Remember to include information about your purposes and lawful basis in your participant information sheets.

Refer to the Information Commissioners Office guidance for further information on the use of 'public interest' as the lawful basis for processing.

It is important to note that although 'public interest' – and not 'consent' - is likely to be the lawful basis under which personal data is held and processed, the ethical and common law requirements of consent are not reduced.

Resources

- Consumer Data Research Centre: The General Data Protection Regulation & Social Science Research

- General Data Protection Regulation: The full text

- Information Commissioner's Office: Guide to the General Data Protection Regulation

- Information Commissioner's Office: Lawful basis interactive guidance tool

- Health Research Authority: Guidance for Researchers
- University of Liverpool data protection webpages
- University of Liverpool Research Ethics Policy
- University of Liverpool Research Data Management Policy
- University of Liverpool Information Security Policy
- University of Liverpool: Getting ready for GDPR training (obligatory training module)