Find out how the data protection principles apply to research

This post will help you better understand UK data protection law in a research context. Read through the post or use the hyperlinks to use as a reference guide.

# Introduction

The UK General Data Protection Regulation (UK GDPR) is a UK law which came into effect on 1 January 2021. It sets out the key principles, rights and obligations for most processing of personal data in the UK. It is based on the EU GDPR (General Data Protection Regulation (EU) 2016/679) which applied in the UK before that date, with some changes to make it work more effectively in a UK context.

The Data Protection Act 2018 sets out the framework for data protection law in the UK. It updates and replaces the Data Protection Act 1998 and came into effect on 25 May 2018. It was amended on 1 January 2021 by regulations under the European Union (Withdrawal) Act 2018, to reflect the UK’s status outside the EU. It sits alongside and supplements the UK GDPR.

The legislation concerns the **processing** (e.g. acquiring, holding, using) of information about individuals (‘**personal data**’).

The aim of data protection law is to balance the rights of individuals to privacy, with the legitimate interests of organisations to process personal data. UK GDPR gives extensive rights to individuals about whom The University of Manchester holds information.

It does not mean that researchers can’t obtain and use personal data, but it does impose legal controls and restrictions that must be adhered to. There are **six data protection principles** that set out the requirements for handling personal data plus a requirement to demonstrateaccountability. We will explore these later in this post.

In the UK the [Information Commissioner’s Office](https://ico.org.uk/)(ICO)upholds information rights and oversees the legislation. Breaches of the UK GDPR may result in investigations by the ICO, potentially leading to significant fines, civil or criminal liability, adverse publicity and could damage your reputation as a researcher. You must also consider the impact that a breach might have on participants, causing them distress or embarrassment. A serious breach could ultimately lead to public distrust and a reluctance to participate in future studies.

UK GDPR is not designed to impede research; considering data protection isn’t an additional burden, much of it is common sense and consistent with applying normal research ethics principles.

# Does your research involve personal data?

## Defining personal data

The definition of personal data is deliberately broad; any information relating to a living person (the ‘data subject’).

A living person is one who can be identified, directly (from the data itself) or indirectly (from the combination of the data with other available data), by reference to an identifier such as a:

* Name
* Identification number
* Location data
* Online identifier.

Or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that living person.

**UK GDPR does not apply to anonymous data:** However, researchers should consider whether or not an individual can be identified even after the usual identifiers have been removed.

## Processing personal data

There are additional considerations when it comes to the processing of personal data. **‘**Processing’ covers the majority of what a researcher might do with personal data, for example:

* Organising, adapting or altering it.
* Retrieving, consulting or analysing it.
* Disclosing, publishing, disseminating or otherwise making it available.
* Deleting or destroying it.

## Special category data

Certain types of personal data are considered to be particularly sensitive and or could be used in a discriminatory way. These data types have been given specific protection within the UK GDPR; they include:

* personal data revealing racial or ethnic origin,
* personal data revealing political opinions,
* personal data revealing religious or philosophical beliefs,
* personal data revealing trade union membership,
* genetic data,
* biometric data (where used for identification purposes),
* data concerning health,
* data concerning a person’s sex life, and
* data concerning a person’s sexual orientation.

Special category information must be processed with additional safeguards in place.

# The six principles of Data Protection

Researchers must process all personal data in accordance with the following principles.

## Personal data must:

1. Be processed lawfully, fairly and in a transparent manner; **(lawful, fair and transparent).**
2. Be collected only for specified, explicit and legitimate purposes, and not be further processed in any manner incompatible with those; **(purpose limitation).**
3. Be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed; **(data minimisation).**
4. Be accurate and, where necessary, kept up to date; **(accuracy).**
5. Not be kept as identifiable data for longer than necessary for the purposes concerned; **(storage limitation).**
6. Be processed securely (integrity and confidentiality).

# The rights of the data subject

Individuals have extensive rights under the UK GDPR, which they may exercise by submitting requests to the data controller processing their data. Data subjects have the following rights: the right of access, rectification, erasure (often referred to as the right to be forgotten), objection, restriction of processing, data portability and rights relating to marketing and profiling.

These rights apply differently to different forms of processing and certain rights may not apply at all in certain circumstances. Research is one such area where there are derogations (exemptions) to the data subject rights.

## Exemptions under the Data Protection Act 2018

## Research and Archiving

GDPR allows for the following rights to be limited within a research context:

* the right of access,
* the right to rectification,
* the right to restrict processing,
* the right to data portability,
* the right to object.

However, **there is no blanket exemption**. Exempting or limiting those rights is possible only if they would:

* **prevent** or **seriously impair the research activity in question** (scientific or historical research purposes or statistical purposes) and only if certain safeguards apply, such as measures to ensure there is data minimisation.

In addition, the exemption and the exceptions only apply:

* if the processing is not likely to cause substantial damage or substantial distress to an individual,
* if the processing is not used for measures or decisions about particular individuals, except for approved medical research,
* if the research results are not made available in a way that identifies individuals.

These additional requirements are set out in section 19, and the exemption at Schedule 2, Part 6 of the [Data Protection Act 2018](https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted).

## Reporting a Data Breach

Compliance with the UK GDPR is a legal requirement; breaches of data protection law may result in investigations, significant fines, adverse publicity, and civil or criminal liability.

A breach leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. If you think personal data has fallen into the wrong hands or has been lost, you must report it immediately.

Organisations have a statutory deadline of 72 hours to report serious breaches to the Information Commissioners Office.

To report a data breach, contact the Information Governance Office immediately by emailing: infosec@listserv.manchester.ac.uk

# What are the rules for transferring personal data around the world?

The EU GDPR primarily applies to controllers and processors located in the European Economic Area (the EEA). This is comprised of the EU states plus Norway, Liechtenstein and Iceland. The UK now has its own version of the GDPR.

Because individuals risk losing the protection of the GDPR if their personal data is transferred to a country with a lower standard of data protection law, both the EU and UK GDPR seek to restrict these transfers unless certain measures or safeguards are in place.

The measures or safeguards most commonly used can be split into four types:

1. Transferring personal data to an approved ‘adequate’ country
2. Standard contractual clauses
3. Ad-hoc transfers of personal data
4. Binding Corporate Rules

Seek advice from the Contracts Office, the Procurement team or the Information Governance Office if your research involves the transfer personal data outside of the UK.

## Privacy Shield

This safeguard operated until Summer 2020. It placed requirements on US companies certified by the scheme to protect personal data and provides for redress mechanisms for individuals and replaced another previous safeguard for the same kind of transfers, called Safe Harbour. The US government Department of Commerce oversaw certification under the scheme. It allowed transfers to be made to US companies that were members of the Privacy Shield scheme. The European Court of Justice ruled that Privacy Shield was invalid in a July 2020 judgement. This ruling, the so-called Schrems II judgement, stated that personal data can no longer be transferred to a US based company under the framework and no new contracts can be entered into that seek to rely on it.

It is likely that the Standard Contractual Clauses will now need to be used for most of these transfers. Because of the Schrems II judgement we must now seek some additional assurance that the other party is able to comply with the SCCs (there is a specific clause relating to the US and another for data importers based in other countries) before we agree to them.

Seek advice from the Contracts Office, the Procurement team or the Information Governance Office if your research involved the transfer personal data to the US or another non-adequate country.

## Location of researcher

For research work at University of Manchester, it does not matter if the research project is taking place in a country outside the UK or EEA, the UK GDPR will apply irrespective of where the data processing is taking place if The University is processing personal data or is the data controller. Local laws may also apply.

# What do I need to consider as a researcher?

## Data Management Plan

The [Data Management Plan](https://www.library.manchester.ac.uk/using-the-library/staff/research/research-data-management/planning/) outlines how a research project will manage data both during the research and after the project is completed. You are asked to add in detail (proportionate to the nature of your research) about what personal data will be collected, processed and stored.

## High risk processing assessments

If your research is likely to involve [high-risk processing](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/examples-of-processing-likely-to-result-in-high-risk/) the relevant researcher or PI may need to complete a research assessment which may ultimately lead to a full Data Protection Impact Assessment being carried out. This will be done in consultation with the Information Governance Office. For more information as to what constitutes ‘high risk’ processing read the following [ICO guidance and examples](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/examples-of-processing-likely-to-result-in-high-risk/).

## Contracts

If your research involves sharing personal data with another organisation (i.e. not just the anonymised outcomes) a contract must be in place. Contact the contracts office for advice.

This will involve agreeing who the ‘data controller’ is and where necessary, who the ‘data processor’ is. In most cases The University will be the controller, but this will be assessed by the legal advisors and the Information Governance Office.

## Participant Information Sheets

Ensure that your participant information sheet and consent forms include sufficient information to meet the UK GDPR requirement of transparency.

## Anonymisation and Pseudonymisation

UK GDPR does not apply to anonymous data; however, researchers should consider whether or not an individual can be identified even after the usual identifiers have been removed. If data can be combined from different sources, it may allow a person to be identified — whether by the research team or by another person. Note that the process of anonymising personal data is covered by UK GDPR.

Pseudonymisation is a method of disguising the identities of individuals to whom information relates. It may involve removing a common identifier and using a pseudonym (e.g. a randomly allocated number), enabling data to be collected about the same individual without recording their identity. Pseudonymising data can be useful in research as a method of applying a safeguard to protect personal data.

# Summary

In this resource we explored Data Protection Law and how it applies to research with human participants.

# Thank you to our contributors

These resources were created in partnership with University of Manchester’s Information Governance team. Special thanks to Liz Skae, Alex Daybank, and Laurence Malbeaux who wrote and advised on the content