

### Summary

- In order to process personal data we need to have a lawful basis for the processing and to have additional grounds for processing special category personal data and criminal offence data.
- For any processing of personal data, we must comply with the Data Protection Principles, but there are several specific provisions/exceptions for research related processing which recognise the importance and special nature of research and ensure that data protection requirements support innovation and the advancement of knowledge.
- To rely on these research provisions, we must ensure that we have appropriate safeguards in place.

### What does research related processing mean in a data protection context?

It covers three types of purpose:

- archiving purposes in the public interest;
- scientific or historical research purposes; and
- statistical purposes.

This guidance focuses on the second of these. The legislation refers to “scientific or historical research” but has a broad definition that covers the full range of academic research, including the arts, social sciences, and humanities which aims to increase knowledge or devise new applications of available knowledge. The [ICO guidance on research](#) provides more detail.

### Lawful basis for processing

When we process personal data, we need to have a lawful basis for that processing. The UK GDPR provides 6 options:



**Consent** – the consent of the data subject to the processing of their personal data



**Vital Interests** – it is vital that specific data are processed for matters of life or death



**Contractual necessity** – processing is needed in order to enter into or perform a contract



**Public task/Public Interest** – public authorities and organisations in the scope of public duties and interest.



**Legal obligation** – the controller is required to process personal data to meet a legal obligation



**Legitimate interest** – There is a weighed and balanced legitimate interest where processing is needed and the interest is not overridden by others

**The lawful basis for most academic research carried out by the University is public task/public interest - processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.** This stems from the powers and duties of a university as set out in statute which include conducting research and publishing the results of that research.

## What about consent?

We obtain consent from participants to take part in a research study and this is an important ethical standard. However, this consent to participate is distinct from consent as a lawful basis to process personal data. UK GDPR consent is usually not the most appropriate lawful basis for data processing because:

- GDPR consent can be withdrawn at any time and it will be difficult or impossible to manage and action the withdrawal of consent in a research context after the initial data collection period; and,
- GDPR consent is not an appropriate lawful basis for processing where there is a power imbalance between the University and the individuals whose data we are processing.

The [ICO guidance on research](#) sets out the position on consent for research in more detail and this may be helpful when dealing with queries from research participants.

## Research conditions for processing Special Category Personal Data and Criminal Offence Data

If we are processing special category personal data, we need to **identify a lawful basis AND a special category personal data condition** (as set out in Article 9 of the UK GDPR).

Article 9 (2)(j) covers the use of special category personal data for research purposes. There is a similar condition for criminal offence data in the Data Protection Act 2018, Schedule 1, condition 4.

We can rely on these special category personal data and criminal offence data conditions if the processing is:

- Necessary for that purpose;
- Subject to appropriate safeguards;
- Not likely to cause someone substantial damage or substantial distress;
- Not used for measures or decisions about particular people (except for approved medical research); and
- In the public interest.

## What does 'necessary' mean?

The special category personal data and criminal offence research conditions require that the processing is 'necessary' for the purpose in question. If we could reasonably achieve the same purpose by less intrusive means, we cannot rely on the conditions. The processing doesn't have to be absolutely essential, but must be a targeted and proportionate way of achieving the purpose.

## When is research-related processing 'in the public interest'?

The special category personal data and criminal offence research conditions state that processing must be in the public interest, but the legislation doesn't define this. The ICO states that we should "broadly interpret public interest in the research context to include any clear and positive public benefit likely to arise from that research" and recognises that this will vary depending on the project. The avoidance of harm to the public will be a key factor. It is the University's responsibility to demonstrate that the research-related processing is in the public interest. More detail in the [ICO Research Guidance](#).

## Data Protection Principles

Personal data shall be:

- a. processed lawfully, fairly and in a transparent manner,
- b. collected for specified, explicit and legitimate purposes,**
- c. adequate, relevant and limited to what is necessary,
- d. accurate and where necessary kept up to date,
- e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed, and**
- f. processed in a manner that ensures appropriate security of the personal data.

There is an additional **Accountability Principle** which is central to UK GDPR. Data controllers are responsible for compliance with the principles and must be able to demonstrate this to data subjects and the regulator.

We must comply with all the principles for all our processing at the University, but two of the principles above (b – the purpose limitation principle, and e – the storage limitation principle) contain some special provisions for research-related processing.

### How the purpose limitation principle applies to research related processing

The principle states that personal data shall be:

*“...collected for specified, explicit and legitimate purposes and not further processed in a manner than is incompatible with those purposes...”*

However, it goes on to say that processing for research purposes will not be considered to be incompatible with the initial purposes.

This simply means that processing data for research-related purposes is compatible with the original purpose.

This applies as long as your intended further processing:

- meets the criteria for one of the research-related purposes;
- is necessary for one of the research-related purposes ;
- is fair and lawful; and
- has appropriate safeguards in place.

If we re-use data that was originally collected for another purpose, the lawful basis that we rely on may be different and will usually be public task/public interest.

The main issue comes when we want to use personal data that was originally collected by consent as we would need to seek fresh consent for any new processing activity, including research. UK GDPR consent must be specific and informed, so using it for a research related purpose without the individuals’ knowledge or agreement would unfairly undermine the informed nature of their original choice.

You can carry out research on anonymised data, even if it was originally collected on the basis of consent as data protection law doesn’t apply to fully anonymised data.

You can also obtain quite broad consent for research as the law recognises that in a research context it isn’t always possible to fully identify the specific research purposes at the time that the data is collected.

## How the storage limitation principle applies to research

The general rule is that we cannot hold personal data indefinitely just in case we might find it useful in the future – the retention period has to be linked to the purposes for which it was collected. However, there is an exception to this rule for research-related processing, meaning that we can keep personal data if we are processing it solely for research or archiving purposes in the public interest. We must have appropriate safeguards in place.

If we are no longer processing the data for any purposes, including a research-related purpose, the data needs to be deleted. There are no data protection restrictions on the retention of anonymised data, but we do need to be sure that the data is properly anonymised.

## What are the appropriate safeguards?

In order to use the research provisions, we need to have appropriate safeguards in place. These protect the rights and freedoms of the people whose personal data we are processing. The legislation explicitly mentions anonymisation and pseudonymisation as potential appropriate safeguards, but there are others that we need to consider too.

### 1. Data minimisation

- The ICO advises that wherever possible, we carry out research using **anonymous** data.
- If it isn't possible to use anonymous data, we should consider whether we could **pseudonymise** the data.
- We should only collect and use personal data which is “adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed”.

2. We may not use the research provisions if the processing is for the purposes of **measures or decisions with respect to particular individuals** (unless the research is approved medical research).

3. We may not use the research provisions if the processing is likely to cause someone **substantial damage or substantial distress**.

- Substantial damage would include both material and non-material harms, such as: financial loss; economic or social disadvantage; physical harm; damage to reputation; loss of confidentiality; or deprivation of rights.
- Substantial distress would include upset, emotional or mental pain. It goes beyond annoyance, irritation, or strong dislike.

4. **Other data protection measures** that we should also have in place include:

- Conducting Data Protection Impact Assessments (DPIAs)
- Taking a ‘data protection by design and default’ approach to data processing for research
- Implementing appropriate security measures
- Good levels of staff training

More detail in the [ICO Guidance on research](#).

### Further Information and Support: Information Governance Team

Sharepoint: <https://sheffieldhallam.sharepoint.com/sites/3037/SitePages/Information%20Governance.aspx>

Email: [DPO@shu.ac.uk](mailto:DPO@shu.ac.uk)