

Contents

Data protection law: managing the rights of participants rights and the interests of researchers	1
Definitions of types of data	2
The lawful bases and conditions for processing personal data	3
The data protection (privacy) rights	3
Privacy rights: when are these available?	4
Applying a research exemption	5
Additional information on privacy rights.....	5
The research derogations for secondary use and long term storage of data.....	5
Lawful basis and condition for the University’s research involving personal data	6
The research safeguards	6
Research safeguards in the University context.....	7
Privacy impact assessments and records of processing activities	7
Further help.....	7

Data protection law: managing the rights of participants rights and the interests of researchers

Specific terms are in italics and explained later in this document

European and UK data protection law i.e. the General Data Protection Regulation (“the GDPR”) and the Data Protection Act 2018 bolsters privacy rights, by giving individuals greater control over their *personal data* and limiting what organisations can do in certain circumstances.

The legislation requires that all *personal data* being collected and analysed be done so in accordance with a specific *lawful basis*. If *special category personal data* are involved, there is an additional step of identifying which *condition* is being used to allow for processing such sensitive data. Both the *lawful basis* and *condition* need to be stated to a research participant in a *privacy notice*.

The legislation also explicitly requires that a *record of processing activities* is kept, requiring documentation of, for example, processing purposes, data sharing and data retention.

To protect research activity that relies on *personal data*, there is provision to limit the *data protection rights* of those participating in research. For example, in many instances *personal data* gathered for research purposes can be kept indefinitely, if *the research safeguards* are in place. The *data protection rights* that are available to such participants will depend on the *lawful basis* and *condition*, and/or on specific *research exemptions*.

The University's researchers will:

1. Always use **public task** as the *lawful basis* of processing and **public interest research** as the *condition* for processing special category data;
2. For ethical reasons, always explicitly provide their participants with the *right to erasure* up to the end of the project's data gathering period, despite the *lawful basis* and *condition* not requiring this, by adjusting the relevant sentences on the template participant information sheet and consent form;
3. Meet the needs of undertaking a *privacy impact assessment* and keeping a *record of processing activities* by completing the ethical review application form;
4. Meet the needs of providing a *privacy notice* by using the template participant information sheet, which communicates the *lawful basis* and *condition* detailed in 1; and
5. Operate in line with *the research safeguards* by following this guidance.

To help researchers understand the above in more detail, this guidance explains:

- Definitions of types of data;
- Lawful bases and conditions for processing special category data;
- Data protection (privacy) rights, applying a research exemption, and the research derogations;
- The research safeguards; and
- Privacy impact assessments and records of processing activities.

Definitions of types of data

Personal data is 'information relating to natural persons who: can be identified or who are identifiable, directly from the information in question; or who can be indirectly identified from that information in combination with other information'. The kinds of information that could result in a natural person being identifiable include the following: names, dates of birth, ID numbers, location data (e.g. GPS), addresses, IP addresses and cookies. Raw and pseudonymised data are subject to the legislation, but data that are irreversibly anonymised or about deceased persons are not.

Personal data might be pseudonymised, meaning they can be indirectly linked to an individual using a 'key'.

Special category personal data are those relating to: race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life, or sexual orientation.

Anonymous data, if irreversibly and truly anonymised, are NOT personal data and are not subject to the legislation.

The lawful bases and conditions for processing personal data

Not all the lawful bases for using personal data are set out here; several are unlikely to apply to research activities. The following have been identified as most relevant.

Lawful basis (for processing personal data)	GDPR Reference	Notes
Consent	GDPR Article 6 1(a)	Seeking an individual's permission.
Public task/delegated authority	GDPR Article 6 1(e)	The University has delegated authority/powers to conduct research. The relevant (enacting) legislation being the Universities (Scotland) Act 1889 when read with the Universities (Scotland) Act 1966; the power being "To regulate and superintend the teaching and discipline of the University and to promote research."

Condition (for processing special category personal data)	GDPR Reference	Notes
Explicit consent	GDPR Article 9 2 (a)	When working with special categories of personal data i.e. information concerning an individual's racial or ethnic origins, political and other beliefs, physical and mental health and sex life, a lawful basis from GDPR, Articles 6 and 9 will be required.
Public interest research in the areas of scientific, or historical, or statistical purposes in accordance with GDPR safeguards	GDPR Article 9 2 (j)	
Substantial public interest grounds based on European Union or UK law	GDPR Article 9 2 (g)	

Consent to participate in research is not the same as *consent as the lawful basis for making use of the personal data of research participants*. A person can be asked to consent to participate in research, but they can also be informed that, if they agree to participate, their personal data will be used for a task in the public interest. The lawful basis for data processing in that instance is not consent.

The data protection (privacy) rights

These can be summarised as:

The right to be informed	Organisations that collect/receive personal data must clearly and fully inform the individuals concerned, normally in writing, normally at the point when personal data is being collected, how their personal data will be used. Typically, in research, this will happen through the details passed to people in a participant information sheet. For some research activities this information can be introduced at a later stage, after research has started, depending on recognised ethical standards.
The right of access	Commonly referred to as subject access or a subject access request, this gives individuals the right to obtain a copy of their personal data as well as other

	supplementary information, including confirmation as to the legal basis used to make use of those data. It helps individuals to understand how and why an organisation is using their personal data, and to understand if that use is lawful.
The right to rectification	If personal data is inaccurate, out of date, or incomplete, individuals have the right to correct, update or complete that data. Collectively this is referred to as the right to rectification. Rectification may involve filling the gaps i.e. to have incomplete personal data completed – although this will depend on the purposes for the processing.
The right to erasure	In certain circumstances people can, at any time, ask for their personal data to be erased from the records held by organisations.
The right to restrict processing	Where the use of personal data is in dispute, for example, there is a claim that personal data are inaccurate, the right to restrict processing may then apply. This means that an individual can limit the way that an organisation uses their personal data. This is an alternative to requesting the erasure of their data.
The right to data portability	Individuals have the right to get some of their personal data from an organisation in a way that is accessible and machine-readable, for example as a csv file.
The right to object	In some circumstances, individuals have the right to object to the processing. If the University agrees to an objection, it must stop using the personal data for that purpose unless it can give strong and legitimate reasons to continue to make use of the data despite the objections that were raised.
Automatic decision making and profiling	Individuals have the right to object to the automatic use of their personal data where this is used to support decision making and profiling. For example, a multiple-choice assessment graded by computer with no human intervention or checking. Presently the University does not have such processes in operation; should it do so then that will be made known in the relevant privacy notice(s).

Privacy rights: when are these available?

The table, below, summarised when privacy rights are available against a lawful basis. This does not take into account research exemptions, which, if applied, would restrict some of these rights.

Type of data	Lawful basis for processing	Data protection rights					
		Access	Rectification	Erasure (right to be forgotten)	Restriction	Data portability	Objection
Personal data	Consent	✓	✓	✓	✓	✓	✓
	Public task/delegated authority	✓					✓
Special category personal data	Explicit consent	✓	✓	✓	✓	✓	✓
	Scientific, historical research purposes, or statistical purposes in accordance with GDPR safeguards	✓					
	Substantial public interest grounds based on European Union or UK law	✓					

The Data Protection Act 2018 contains provision to exempt the following privacy rights, where *the research safeguards* (see, below) are in place:

- The right of subject access;
- The right to rectification;
- The right to restrict processing; and
- The right to object.

The exemptions can only be lawfully applied, and the rights restricted, where providing a right would be likely to render impossible or seriously impair the research.

Applying a research exemption

Contact the Information Assurance and Governance team: dataprot@st-andrews.ac.uk, who will establish whether an exemption can be successfully applied or otherwise before responding to all concerned. Requests will be logged, and the outcomes held on record. If Individuals believe that their data protection rights have not been provided, they have the right of complaint to the University and then to the Information Commissioner's Office. The University is required to maintain evidence as to how requests to exercise data protection rights were managed.

For example, an individual participating in an experiment to establish degrees of colour blindness may ask their responses to an experiment to be deleted. The experiment responses are recorded and held against a participant number. Participant numbers can be linked to the names of the individuals who contributed to the research, meaning that the responses remain their personal data.

The request for deletion is made 30 months after the experiment has concluded; a journal article has been submitted and is in the final stages of peer review. It was determined that (a) granting the request would undermine the research process, as the sample size would be altered having a significant effect on the findings and (b) there is no right of erasure in this instance, as the lawful basis for the research is public task.

Additional information on privacy rights

Consult University website: <https://www.st-andrews.ac.uk/terms/data-protection/rights/> or email dataprot@st-andrews.ac.uk.

The research derogations for secondary use and long term storage of data

Data protection law also recognises that where personal data are to be used for research that, subject to the application of the research safeguards:

- Personal data can be used for research purposes, even if that was not the original reason for collecting those data; and
- It may be necessary to retain personal data for an indefinite time.

When designing research and/or explaining to participants how their personal data will be used, the above elements may be important.

Lawful basis and condition for the University's research involving personal data

Lawful basis	GDPR Reference	Notes
Public task/delegated authority	GDPR Article 6 1(e)	The University has delegated authority/powers to conduct research. The relevant (enacting) legislation being the Universities (Scotland) Act 1889 when read with the Universities (Scotland) Act 1966; the power being "To regulate and superintend the teaching and discipline of the University and to promote research."
Public interest research in the areas of scientific or historical or statistical purposes in accordance with GDPR safeguards	GDPR Article 9 2 (j)	
Substantial public interest grounds based on European Union or UK law	GDPR Article 9 2 (g)	

If you have questions about the lawful basis for making use of personal data, and/or special category personal data, please email dataprot@st-andrews.ac.uk.

The research safeguards

These include, and are to be applied as appropriate, where compatible with the research process:

- The research will not be likely to cause substantial damage or distress to participants.
- Other than for medical research, personal data should not be used to make a decision about an individual.
- The principle of data minimisation is followed i.e. only the minimal amount of data necessary to complete a specific objective is collected.
- Exemption of privacy rights in relation to research is only undertaken where to provide a right(s) would render impossible or seriously impair research.
- Personal data should be pseudonymised - personal data should not be used where the research purpose can be fulfilled by working with anonymised data.
- Information security measures are in place, such as encryption of devices and working with up to date antivirus software.
- Where using special category personal data an additional safeguard is required i.e. the research must be in the public interest (demonstrated over and above using 'task in the public interest' as the lawful basis). It is assumed that all research that has passed through an ethical review process will be in the public interest.

Research safeguards in the University context

The safeguards will invariably be in place where University policy, regulation and procedures concerning:

- Ethical approval and good research practice have been followed, and there has been no material change to the research design and operation and/or any conditions set have been met and continue to be addressed; and
- Information classification and the use of ICT are in place to protect personal data. Please see *Keeping research data of human participants secure, when working with Information Communication Technologies (“ICT”)*.

Privacy impact assessments and records of processing activities

The legislation requires that certain activities require a privacy impact assessment (PIA) to be undertaken as part of planning relevant activity, which involves asking questions relating to the following seven principles: lawfulness, fairness and transparency (identify a lawful basis for processing the data); purpose limitation (identify a clear purpose for processing the data); data minimisation (limit the data being processed to that which is adequate, relevant and necessary); accuracy (ensure that the data held are not incorrect or misleading as to any matter of fact); storage limitation (only keep the data for as long as is justifiable); integrity and confidentiality (protect data with appropriate security measures); and accountability (the University has overarching responsibility for legal compliance, and should provide policies, processes and guidance that support employees to meet these requirements). Drawing on guidance from the Information Commissioner’s Office, the University has decided that all research involving data defined as ‘personal data’ in the legislation should be subject to the equivalent of a PIA.¹

The legislation also explicitly requires that processing activities are documented, requiring that records are kept on, for example, processing purposes, data sharing and data retention.²

Further help

This is a short guide to introduce some basic data protection requirements, noting how these may impact on research activities. For additional information and/or help please contact:

- The University Data Protection Officer: email dataprot@st-andrews.ac.uk
- University Teaching and Research Ethics Committee (UTREC): email utrec@st-andrews.ac.uk
- Research and Innovation Services: email rpo@st-andrews.ac.uk
- Research Data Management: email research-data@st-andrews.ac.uk

¹ <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/examples-of-processing-likely-to-result-in-high-risk/>

² <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/>