University of Dundee

Data Protection and Research - Guidance

Our students, colleagues and partners all trust the University with their personal data. The General Data Protection Regulation enhances our legal obligations in this domain. Meeting those obligations is a key component in conducting ethical research and meeting the requirements placed upon us by our funders.

Contents

1. What is GDPR?

GDPR is the General Data Protection Regulation. It came into force along with a new UK **Data Protection Act** on 25 May 2018. Together they replaced the previous Data Protection Act entirely. They provide the legal framework for holding and using personal data and set out the rights of individuals in respect of their data.

2. What has changed?

The changes in GDPR cover every aspect of our interaction with personal information.

Changes include

- New definition of personal data
- New definition of sensitive personal data
- Revised data protection principles
- 'Accountability' principle
- Records of processing activities
- Data Protection Impact Assessments
- Changes to 'lawful' processing
- Changes to rules around consent
- Individual rights – the right to be informed
- Individual rights – the right of access
- Individual rights – the right to rectification
- Individual rights – the right to erasure
- Individual rights – the right to restrict processing
- Individual rights – the right to data portability
- Individual rights – the right to object
- Individual rights –automated decision making and profiling
- Breach notification
- Transfer of data outwith the EU

- New (stricter) penalties

3. What are the data protection principles?

Article 5 of GDPR sets out the principles governing the processing of personal data. Remember that 'processing' in this sense includes just having personal data. You don't have to be doing anything with it for the rules to apply.

The data protection principles

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f) 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 ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

GDPR also gives us updated definitions of 'personal data' and 'special categories of personal data'. The rules for processing special category data are stricter than those for personal data.

4. What is personal data?

Key definition - personal data

Personal data is '*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*'.

An obvious identifier (such as a name) can make information personal data, but remember that other elements can identify someone (especially when used in combination). This is particularly important in research where seemingly anonymous data can identify someone when used in combination with other information.

5. What is special category personal data?

Key definition - special categories of personal data

Special categories of personal data are what we used to know as 'sensitive' personal data. However, note that the processing of special categories of personal data is normally prohibited. We will look at the rules on lawful processing of special categories of personal data shortly.

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

Please also note that processing of criminal conviction data requires special care and you should seek advice if your research involves that type of information.

The first data protection principle deals with 'lawfulness, fairness and transparency'. **Lawful** has a specific meaning in this context.

6. What makes the use of personal data or special category personal data 'lawful'?

Lawful processing of personal data

For the processing of **personal data** to be lawful, at least one of the following must apply:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) 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;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

The University, as a Scottish Public Authority, cannot normally use (f) and claim that processing is lawful due to its 'legitimate interests'.

Lawful processing of special category personal data

For the processing of **special categories** of personal data to be lawful, one of the following must also apply:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition...[on processing special categories of personal data]...may not be lifted by the data subject;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of 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;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to...[relevant]... conditions and safeguards...;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(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.

6.a. Why might the use of personal data and special category personal data in research be lawful?

It is important to think about why research activity is lawful to make sure our approach is appropriate ***and*** so that we can give the right information to our research participants. We will look at 'fairness and transparency' in a moment.

At the University of Dundee, the normal basis for the lawful processing of personal data in research is likely to be that ***'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'.***

The University's Royal Charter notes that '*the objects of the University shall be to advance and diffuse knowledge, wisdom and understanding by teaching and research and by the example and influence of its corporate life'* and gives it specific powers in relation to the conduct of research here. When conducting research activity that involves processing personal data the University will normally be acting under that official authority or performing research in the public interest.

The normal basis for the lawful processing of special categories of personal data in research is likely to be that ***'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'.

The requirements to use Article 89(1) as a lawful basis for using special category data in research

Article 89(1) of GDPR, in combination with some sections of the Data Protection Act 2018, provides for research to be conducted using special categories of personal data, subject to specific safeguards and protections:

- technical and organisational security measures must be in place to ensure the security and integrity of the data. These measures should be documented. Technical security includes things like physical security, encryption, access controls etc. Organisational measures include things like research contracts and associated data sharing/processing agreements, research data management plans etc. Please seek advice on these areas in the research design phase;
- the minimum amount of special category personal data must be used to achieve the aims of the research. You must be able to evidence that your research only uses the minimum amount of personal data and special category personal data;
- where you are able to work with anonymised data you must do so;
- where you cannot use anonymised data, you must use pseudonymised data if you are able. You should keep evidence of why you are unable to work with anonymous data;
- the use of identifiable data should be the last resort rather than a preferred option. If you are unable to use pseudonymised data you should seek guidance on whether the use of identifiable data is appropriate and keep evidence of why that was the case;
- if you are working with identifiable or pseudonymised data, you must move to anonymised data as soon as you are able;
- your research must not cause any individual substantial damage (normally actual or financial harm);
- your research must not cause any individual substantial distress (normally emotional or mental anguish or harm);
- you may not process data in your research to make decisions or take measures in relation to any individual*;
- you many not identify any individual in the results or statistical outputs of your research. Please keep this in mind when reviewing datasets for release as open data.

If you can't meet any of these requirements then you must seek additional advice before proceeding with your research from School Ethics Committees, UREC or TASC as appropriate. Information

Governance (dataprotection@dundee.ac.uk) and the Research Data Management team in the University Library can also help as needed.

*Medical research is a little different in this respect. Please seek guidance from TASC and Information Governance.

7. What makes the use of personal data 'fair and transparent'?

Fairness and transparency means that we must tell people what is happening to their information. This is done using a 'privacy notice'. In a research context, the provision of the mandatory information required by GDPR may be done as part of participant information sheets. Whichever approach is used, the information on how their data will be processed should be given to individuals at the point of collection. Where data is received from a third-party (perhaps shared with the University by a research partner), slightly different rules apply. Please seek advice from Information Governance when working with external partners.

7.a. What must be included in 'privacy notices' or participant information sheets?

People must be given:

- *the identity and the contact details of the controller and, where applicable, of the controller's representative;*
- *the contact details of the data protection officer, where applicable;*
- *the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;*
- *...the recipients or categories of recipients of the personal data, if any;*
- *where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation...[the basis for that transfer and the documentation/safeguards etc in place for that transfer];*
- *the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;*

- *the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;*
- *the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;*
- *the right to lodge a complaint with a supervisory authority;*
- *whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract;*
- *whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;*
- *the existence of automated decision-making, including profiling...and...meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.*

The Information Commissioner's Office publish guidance on this here - https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/.

The University has templates to help organise privacy notices online here - https://www.dundee.ac.uk/information-governance/dataprotection/.

8. Should we use consent as a lawful basis for processing personal data or special category personal data in research?

Consent remains fundamental to ethical research practices and consent to participate and/or consent to use particular contact methods will be essential to many projects.

Consent may also be the basis for lawful processing of personal data. However, if you are going to use consent you must ensure that it is:

- freely given (ie if the person has no option but to take part, they cannot 'consent' to doing so);
- informed;
- specific (ie if you have more than one aspect to your project you are likely to need granular consent for each element of your research activity);
- unambiguous (you are clear on what is being consented to);
- the result of a positive action (ie a signature, a tick in a box, the completion of a declaration etc. You cannot rely on pre-ticked boxes or statements to the effect that 'if we don't hear from you we will accept that as consent and...').

Importantly, you must be able to evidence the consent on which you are relying.

Finally, you must be able to manage the consent process. Specific and granular consent means that an individual could withdraw their consent for a single aspect of your research activity, whilst leaving

consent for other aspects in place. It's important to consider how you would manage the administrative implications of that or how you would extract a single person's information from your project entirely if consent is your lawful basis for processing their data.

The Information Commissioner's Office provide guidance on consent under GDPR here - https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/.

Throughout the proceeding sections of this resource, we've stressed the importance of keeping records to evidence compliance with GDPR. Much of what is required is crucial to developing privacy notices or participant information sheets and communicating fairly and transparently with individuals. Keeping records of our activities is also a requirement of GDPR and helps to meet the 'accountability' principle mentioned earlier.

9. What records should we keep about our use of personal data in research?

Article 30 of GDPR sets out what should be kept as 'records of processing activities':

- *the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;*
- *the purposes of the processing;*
- *a description of the categories of data subjects and of the categories of personal data;*
- *the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;*
- *where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and...[where appropriate] the documentation of suitable safeguards;*
- *where possible, the envisaged time limits for erasure of the different categories of data;*
- *where possible, a general description of the technical and organisational security measures...[being used].*

As you can see, this is very similar to the information required for a privacy notice and to meet the requirements of Article 89(1) when conducting research using special category data.

In practice, this information is likely to be held in your research design documentation, your ethics approval paperwork and your research data management plan. However, if you have not covered all of the bullets above, please seek guidance from Information Governance on how those elements might be captured in your research information.

Remember also that if you are relying on consent for any aspect of your project, you will need relevant supporting evidence for that element of your work too.

10. What is a data protection impact assessment and when should I use one?

Data Protection Impact Assessments detail the personal data used in any process, project or system, the associated privacy risks and their mitigation. They are mandatory for all high-volume or high-risk processing of personal data.

In a research context, your ethics submission should include the elements of a DPIA. UREC have made this a standard part of the University's ethics forms. As part of your ethics submission you will be asked to consider why your research project is lawful, what privacy risks it creates and how those risks have been mitigated.

Mitigation will normally include technical controls (such as the use of encrypted devices) and organisational controls such as research contracts, partnership agreements and or data sharing/processing agreements. These controls can also be captured in your research data management plan.

11. What technical measures can I use to safeguard personal data in research?

The technical controls deployed will vary by project, but good basic data security applies to everyone.

UoD devices for UoD data

- Strong passwords (minimum 14 chrs)
- Encryption
- Up to data anti-virus software

Devices managed by UoD will meet the correct standard of password-protection, encryption etc.

Where personal mobile telephones or tablets are used with University data, they must have the Company Portal app installed.

UoD systems for UoD data (ie you may not store, transfer or collaborate on projects using personal data on non-UoD provided or reviewed and approved services and systems)

Have you thought about where your data is stored or transferred, how and with what safeguards? What are the long term requirements for storage or use beyond the life of the project? Have you build these elements into your research data management plan (see below)? Common places for the storage of research data include:

- Correctly permissioned and secured UoD server space
- UoDIT approved cloud storage and/or collaboration tools (such as those provided via Office 365)

- Data safe havens (such as HIC)

Other means of storage or transfer may be appropriate, but they should be reviewed and accepted by IG, UoDIT, the research data management team in LLC during the research design phase.

Don't forget physical security measures

Is data locked away when not in use? Are offices locked when empty? Are desks kept clear when unsupervised? Are portable devices locked away when not being used?

12. What organisational measures can I use to safeguard personal data in research?

As with technical controls, organisational controls will be project-specific. However, certain common elements are likely to apply.

Contractual controls

These may be research contracts negotiated via RIS, contracts with suppliers managed via Procurement, contracts or agreements with funders or collaboration or consortia agreements between partners. The common element in terms of GDPR is that is we are sharing data with another person or organisation or a third party is processing data on our behalf (remembering that 'processing' includes everything from another party simply holding data on behalf of UoD). Our agreements must therefore include specific data protection controls.

Data protection controls may be contained within the a principal contract or as part of an additional data processing or sharing agreement in support of that contract. Using the right contractual controls is also essential when working with **international partners**. You can find guidance on international transfers of personal data on the University's website.

The University's Legal team have prepared style agreements for data sharing or processing. Please seek guidance from Information Governance in the first instance on how they should be applied.

Research Data Management Plans

Research data management planning is a key element of research design and a requirement of many funders. From a data protection perspective it helps to identify personal data risks and their mitigation and forms a major element of our 'records of processing activities' for research projects. The RDM team in the LLC publish policies and guidance in this domain.

Working through the RDM process will also help to ensure that the requirements concerning data minimisation, anonymisation/pseudonymisation and data security are considered and documented per the requirements noted above.

Ethical approval

Another major element of our records of processing actives in research involving personal data or human participants is ethical approval. Information on research ethics at the University is linked online. Working through the ethics process also helps to fulfil the data protection impact assessment requirement of GDPR (along with RDM plans) by identifying privacy risks and how they will be mitigated.

13. What rights do data subjects have in respect of my research data?

GDPR gives data subjects (ie the people about whom identifiable personal data is processed) a series of rights in respect of their personal data

- Article 15 - Individual rights – the right of access (to an individual's own personal data);
- Article 16 - Individual rights – the right to rectification (the right to have inaccurate personal data corrected);
- Article 17 - Individual rights – the right to erasure (the right to have personal data deleted where there is no longer a lawful basis for its continued use);
- Article 18 - Individual rights – the right to restrict processing (the right to limit the purposes for which personal data can be used);
- Article 20 - Individual rights – the right to data portability (the right to receive a copy of personal data held in systems in a common machine-readable format so that it can be used elsewhere);
- Article 21 - Individual rights – the right to object (to how or why personal data is being used);
- Article 22 - Individual rights – rights related to automated decision making and profiling (where personal data is used to profile people for specific purposes (eg segmenting a particular group of people on the basis of particular characteristics) or where personal data is processed automatically to make decisions concerning individuals).

It is important that researchers recognise that these rights exist so that they can respond appropriately if anyone contacts them wishing to exercise their rights in respect of a research project. Should that happen, please refer them to dataprotection@dundee.ac.uk and Information Governance will assist researchers with the management of personal data rights requests.

Although these rights exists, there are limits upon their application (ie they do not apply in all circumstances) and there are specific limits in respect of research. Researchers should refer to Information Governance when individuals wish to exercise their personal data rights. However, the notes below are provided for information concerning some of the limitations that apply to personal data rights in a research context.

Article 89 of GDPR limits the applicability of the following rights, provided that the data is processed for research and the appropriate safeguards are in place:

- Article 15 - Individual rights – the right of access
- Article 16 - Individual rights – the right to rectification
- Article 18 - Individual rights – the right to restrict processing (the right to limit the purposes for which personal data can be used);
- Article 21 - Individual rights – the right to object (to how or why personal data is being used).

GDPR, Article 89

1. Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to ***appropriate safeguards****, in accordance with this*

*Regulation, **for the rights and freedoms of the data subject**. Those safeguards shall ensure that **technical and organisationalmeasures** are in place in particular in order to ensure **respect for the principle of data minimisation**. Those measures may include **pseudonymisation**provided that those purposes can be fulfilled in that manner. Wherethose **purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner**.*

*2. Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in **Articles 15, 16, 18 and 21** subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.*

3. Where personal data are processed for archiving purposes in the public interest, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18, 19, 20 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

4. Where processing referred to in paragraphs 2 and 3 serves at the same time another purpose, the derogations shall apply only to processing for the purposes referred to in those paragraphs.

The required safeguards are provided in the Data Protection Act 2018.

Data Protection Act 2018, Section 19

*19. **Processing for archiving, research and statistical purposes: safeguards***

(1)This section makes provision about—

(a)processing of personal data that is necessary for archiving purposes in the public interest,

(b)processing of personal data that is necessary for scientific or historical research purposes, and

(c)processing of personal data that is necessary for statistical purposes.

*(2)Such processing **does not satisfy** the requirement in Article 89(1) of the GDPR for the processing to be subject to appropriate safeguards for the rights and freedoms of the data subject if it is **likely to cause substantial damage or substantial distress to a data subject**.*

*(3)Such processing **does not satisfy** that requirement if the processing is **carried out for the purposes of measures or decisions with respect to a particular data subject**, unless the purposes for which the processing is necessary include the purposes of approved medical research.*

The Data Protection Act 2018 also sets out some additional requirements concerning the limitation of the personal data rights noted above:

Data Protection Act 2018, Schedule 2, Part 6

27(1)Thelisted GDPR provisions do not apply to personal data processed for—

(a)scientific or historical research purposes, or

(b)statistical purposes,

to the extent that the application of those provisions would prevent or seriously impair the achievement of the purposes in question.

(2)For the purposes of this paragraph, the listed GDPR provisions are the following provisions of the GDPR (the rights in which may be derogated from by virtue of Article 89(2) of the GDPR)—

(a)Article 15(1) to (3) (confirmation of processing, access to data and safeguards for third country transfers);

(b)Article 16 (right to rectification);

(c)Article 18(1) (restriction of processing);

(d)Article 21(1) (objections to processing).

(3)The exemption in sub-paragraph (1) is available only where—

*(a)**the personal data is processed in accordance with Article 89(1) of the GDPR (as supplemented by section 19), and***

*(b)as regards the disapplication of Article 15(1) to (3), the **results of the research or any resulting statistics are not made available in a form which identifies a data subject.***

What does that mean?

That means that the safeguards we looked at in respect of the lawful processing of special category personal data earlier, also limit the applicability of personal data rights in respect of personal data processed for research, provided that they are applied properly:

- technical and organisational security measures must be in place to ensure the security and integrity of the data. These measures should be documented. Technical security includes things like physical security, encryption, access controls etc. Organisational measures include things like research contracts and associated data sharing/processing agreements, research data management plans etc. Please seek advice on these areas in the research design phase;
- the minimum amount of special category personal data must be used to achieve the aims of the research. You must be able to evidence that your research only uses the minimum amount of personal data and special category personal data;
- where you are able to work with anonymised data you must do so;
- where you cannot use anonymised data, you must use pseudonymised data if you are able. You should keep evidence of why you are unable to work with anonymous data;
- the use of identifiable data should be the last resort rather than a preferred option. If you are unable to use pseudonymised data you should seek guidance on whether the use of identifiable data is appropriate and keep evidence of why that was the case;
- if you are working with identifiable or pseudonymised data, you must move to anonymised data as soon as you are able;
- your research must not cause any individual substantial damage (normally actual or financial harm);
- your research must not cause any individual substantial distress (normally emotional or mental anguish or harm);

- you may not process data in your research to make decisions or take measures in relation to any individual*;
- you many not identify any individual in the results or statistical outputs of your research. Please keep this in mind when reviewing datasets for release as open data.

*Medical research is a little different in this respect. Please seek guidance from TASC and Information Governance.

What about the right to erasure? Will I have to delete my research data upon request?

No. Where deletion would make the research impossible or impair the achievements of the research significantly, the right to erasure is limited. However, that would have to be explained to the data subject per the terms of the legislation, so please contact Information Governance for support if anyone contacts you requesting the erasure of their data.

The limitation on the right to erasure is detailed in Article 17, S.3(d) of GDPR.

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to ***render impossible or seriously impair the achievement of the objectives of that processing****;*

And data portability? Do I have to provide information in a machine-readable format?

Not as long as your lawful basis for processing personal data is 'the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller', which is the University's normal recommended lawful basis for research.

However, if you have used consent as your lawful basis for processing personal data or special category personal data, the right to data portability would apply.

(The right to data portability also applies if the lawful basis for processing personal data is further to a contract with the data subject, although this is less likely in a research context.)

What else do I need to know?

14. How do I report data incidents?

The Information Commissioner's Office 'Guide to the General Data Protection Regulation' defines a data breach as

a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

...

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data

or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

If you think the something inappropriate may have happened (or still be happening) with personal data, it is imperative that you notify Information Governance immediately (dataprotection@dundee.ac.uk).

The quicker the University is aware of a problem, the greater the opportunity to put mitigation in place.

Some very significant decisions also have to be made within 72 hours of the University becoming aware of problem (ie from when you first noticed or were made aware of an issue).

15. Does all this really matter?

Yes. The University has a moral as well as legal obligation to protect personal data. Not doing so can have significant consequences for the individuals who have trusted us with their data, the University (regulatory fines of up to 4% of annual turnover or c.£17,000,000 (whichever is higher)) and for our colleagues in respect of the requirements of the University and the ways that data protection laws can impact them personally. The Data Protection Act 2018 does include a series of criminal offences for things like unlawfully obtaining personal data, re-identifying previously de-identified data or altering data to prevent data subjects accessing their rights. The Crown Prosecution Service publish information on criminal offences on their website.

16. Where can I get help?

For data protection matters, please contact Information Governance first. However, for specific guidance on the areas they cover, please follow the links below.

- Information Governance
- Research Data Management, LLC
- RIS
- TASC (clinical research)
- UREC (non clinical research)
- Legal
- Procurement
- UoDIT

17. Checklist for researchers

- I know what personal data and special category data are required for my project
- I know why it's lawful for me to use that data
- I know how the data will be stored and transmitted securely

- I know what devices will capture, process or access the data and how they are secured
- I have the right agreements in place to govern my relationships with partners, funders and processors and the associated sharing and/or processing of personal data
- I have prepared the right information to communicate what's happening to personal data and why to my research participants, and I know how that information will be communicated to them
- I am using the minimum amount of data necessary for project (and I can evidence that)
- I will not identify anyone in the outputs of my research (and I know how I will achieve that)
- I am not making decisions about individuals with my research data
- I know what to do if anyone makes a personal data rights request
- I know what to do if I think we have had a a data incident
- I have captured all the necessary requirements in my research data management plan and ethics application

Attribution