Research and Innovation Services

General Data Protection Regulation (GDPR) Guidance for Research

The EU General Data Protection Regulation (GDPR) comes into force on 25th May 2018. It will be complemented by a new UK Data Protection Act to replace the 1998 Act.

This document provides practical guidance on the new legislation with respect to research involving person-based data (personal data).

Contents

1. Context

The GDPR adopts a "broad" definition of research, encompassing the activities of public and private entities alike. The GDPR aims to encourage innovation, as long as organisations implement appropriate safeguards.

It should be noted that actions required to comply with the GDPR do not replace or supersede actions that would be required under any other framework such as ethical approval – **they must exist together**.

Controller - A 'controller' determines the purposes and means of processing personal data, and is also jointly responsible for the personal data that is conducted under its auspices. In the context of research the controller can be considered to be both the University, and the lead researcher (who has responsibility for the governance of the data collected as part of the research project they are leading).

Processor - A 'processor' is responsible for processing personal data on behalf of a controller. These can be third parties, for example an external data repository, survey site, and possibly someone such as an external transcriber of qualitative data.

Under the GDPR, in order for the processing of personal data in research to be legal, both criteria below must be satisfied:

1 A **legal basis** to process the personal data under the GDPR must be identified and documented – this is discussed in section 3

2 Any other relevant legal frameworks that need to be met must be satisfied, such as ethical approval (common law duty of confidentiality).

2. Ensuring Compliance – A Starting Point

2.1 GDPR Research Data Registration

Any researcher who wishes to process personal data as part of their research must complete the **Research Data Registration form**.

NB This applies to data held in any form, including paper, tapes, audio, video, CCTV, and Microfiche, as well as data held on electronically.

2.2 Compliance Principles

When processing personal data for purposes relating to research, individuals must comply with the Data Protection Policy and these principles:

- Participants providing their data will receive a Privacy Notice when their data is collected.
- To process personal data the researcher must have a lawful basis.
- When undertaking research involving personal data the individual must complete the Research Registration Form prior to commencing their research.
- The University requires that personal data processed (collected/stored/destroyed) as part of any research project is processed using University approved systems only.
- Personal data must be kept secure at all times
- When collecting personal data, the minimum amount of personal data will be collected that is necessary to undertake the research
- Participants must be notified of the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period
- Wherever possible data should be collected, stored or handled in an anonymous form. If that is not possible, personal data should be pseudonymised and/or processing kept to a minimum
- Where third parties are used to process personal data on behalf of the Researcher, formal written agreements with all third parties who handle personal data on its behalf (data processors). This includes companies or individuals offering: a transcription service, to store information provision of survey tools.
- If a researcher is using a third party to collect or process personal data on its behalf (a 'data processor'), there must have a written agreement with that third party
- Researchers may also need to share personal data with other data controllers (e.g. collaborative projects with other HEIs). Joint controllers will need to have agreements or protocols in place, which set out their respective obligations for data protection compliance.
- Data Protection Impact Assessment must be completed for any project that would be likely to pose a 'high risk' to the rights and freedoms of individuals.
- Researchers must keep records to be able to demonstrate compliance with data protection laws. This would include keeping records relating to consent (if it is relied upon as a lawful basis), copies of fair processing notices agreed by individuals, copies of DPIAs where appropriate and any agreements relied upon.

Further guidance on these areas can be found on The Hub or the University Data Compliance webpages, including 'GDPR guidance for Research'.

If you require further information or have any questions then please read the remainder of this document and contact: Rhys Davies, the Information Compliance Officer.

3. When Does the GDPR Apply?

The GDPR is relevant to research that seeks to collect or process personal data. The data can be obtained directly from a participant or obtained via a third party.

'personal data' means 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

Truly **anonymised** datasets, in which individuals are no longer identifiable (not pseudo anonymised or coded) are exempt from European data protection law. However, the action of anonymising data implies that personal data has **already** been collected/processed and this will have already required compliance with the GDPR.

For further information on Anonymisation please read the ICO Guidance - https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf

4. Principles of GDPR that relating to the Processing of Personal Data

Principle 1 Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject..." GDPR, Art.5(1)(a)
Principle 2 Personal data shall be 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'); GDPR, Art.5(1)(b)
Principle 3 Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'); GDPR, Art.5(1)(c)
Principle 4 Personal data shall be 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');GDPR, Art.5(1)(d)
Principle 5 Personal data shall be 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'); GDPR, Art.5(1)(e)
Principle 6 Personal data shall be 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') GDPR, Art.5(1)(f)

3.1 Fair Processing

Principle 1

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject..." GDPR, Art.5(1)(a)

Being transparent and providing accessible information to individuals about how you will use their personal data is a key element of the EU General Data Protection Regulation (GDPR). The most common way to provide this information is in a **privacy notice**.

The EU General Data Protection Regulation (GDPR) includes rules on giving privacy information to data subjects in Articles 12, 13 and 14.

The GDPR includes a longer and more detailed list of information that must be provided in a **privacy notice** than the Data Protection Act does. There are also some differences in what researchers are required to provide, depending on whether they are collecting the information directly from data subjects or obtaining the data via a third party.

For the avoidance of doubt - researchers should ensure that there is an appendix to their participant information sheet (or equivalent) that provides all information required within a privacy notice. The University is required to make an institutional level 'research' privacy notice available on its Data Compliance webpages.

There are **Privacy Notice** templates available from the Data Protection pages on The Hub.

3.1.1 When personal data is obtained directly from the data subject

When personal data is obtained from a data subject, then a **controller** must provide information to the data subject, at the latest, at the time it is obtained. Data has been obtained from a data subject if the (data) controller obtains the data directly from the data subject.

These scenarios (not exhaustive) are examples of where data is **directly** obtained from the participant:

- completion and return of a questionnaire or survey
- taking part in an interview or focus group
- involvement in an intervention
- recording observations, measurements, or obtaining a sample

The information that must be provided when data is obtained directly from the data subject includes:

(A) Name of controller and contact details (including of data protection officer)
(B) Purposes of the processing, as well as the lawful basis (see section 2.2)
(C) The recipients or categories of recipients of the personal data, if any
(D) The period for which the personal data will be stored
(E) The data subject's rights, including, where processing is based on consent, the right to withdraw consent at any time. Please refer to section on consent discussed later.
(F) The right to lodge a complaint with the ICO
(G) Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data
(H) Any automated decision-making, and, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject
(I) How appropriate or suitable safeguards are achieved in relation to any personal data transferred out of Europe

3.1.2 When personal data is not obtained directly from the data subject

Where personal data is to be used by a researcher but they have not obtained the data directly from the data subject themselves, relevant information must still have been given to the data subject by the original data controller that is supplying the data to the researcher. The receiving Controller also has responsibilities to provide information.

> For example - if a researcher asks the participant's permission to receive personal data held by another controller, e.g. a university researcher asks permission to receive data held by another University or NHS Trust, then the personal data will not have been obtained directly from the data subject directly even though their permission to access has been obtained.

The information that must be provided where data is not obtained from the data subject is slightly different. Where the data is obtained from a third party, then the **controller** receiving the data must provide the following information to the data subject unless they are eligible for a research exemption.

The information that must be provided when data is obtained from a third party:

(A) Name of controller and contact details (including of data protection officer)
(B) Purposes of the processing, as well as the legal basis (see section 2.2)
(C) The categories of personal data concerned
(D) The recipients or categories of recipients of the personal data, if any
(E) The period for which the personal data will be stored
(F) The data subject's rights, including, where processing is based on consent, the right to withdraw consent at any time
(G) The right to lodge a complaint with the ICO
(H) The source from which the personal data originate, and if applicable, whether it came from publicly accessible sources
(I) Any automated decision-making, and, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject
(J) How appropriate or suitable safeguards are achieved in relation to any personal data transferred out of Europe

This information should be provided within a reasonable period. Specifically;

- Within one month, OR
- If the personal data are to be used to contact the data subject, then at the latest at the time of contact, OR
- If disclosure to another recipient is envisaged, e.g. to a researcher employed by another controller, then at the latest when the personal data are disclosed.

NB: If research purposes were not a purpose for which the data were obtained by the original controller, then the relevant information should be provided prior to processing for research purposes.

3.1.3 Research Exemption - provision of information to data subjects

Where personal data is **not** obtained directly from a data subject, then the requirement to provide information does not apply where:

(1) The data are processed consistent with the following safeguard in place:

- Technical and organisational measures that respect the principle of data minimisation are in place. Where possible this requires that:

  - personal data is pseudonymised, and
  - the research activity is conducted without using identifiable data.

AND

(2) The provision of **privacy notice** information proves *impossible* or would involve a *disproportionate effort*. This may be assessed prospectively, **OR**

(3) The provision of the information is likely to render impossible or *seriously impair* the achievement of the objectives of that processing.

It is the **controllers** responsibility to decide which, if any of these circumstances apply and researchers must be able to demonstrate how any of the circumstances are applicable. Therefore, where there is doubt please contact the Data Compliance Officer.

> *Impossible or disproportionate effort* **-** When assessing whether providing information to data subjects proves impossible or would involve a disproportionate effort, "the number of data subjects, the age of the data and any appropriate safeguards adopted should be taken into consideration".
>
> *Impossible or seriously impair* **-** If providing information would undermine the possibility of valid research results, then the provision of information would be likely to render impossible or seriously impair the achievement of the research objectives. When establishing whether providing information would undermine the possibility of valid research results, then appropriate alternate methods of analysis should be considered.

3.1.4 Research Exemption and Public Transparency

When personal data have not been obtained directly from a data subject, and there is no responsibility to provide the relevant information to a data subject due to the operation of a

research exemption then the **controller** must make the information publicly available (and take any appropriate measures to protect the data subject's rights and freedoms and legitimate interests). Therefore, where there is doubt please contact the Data Compliance Officer.

3.1.5 Further Aspects of Fair Processing

Being transparent by providing a privacy notice is an important part of fair processing. You can't be fair if you are not being honest and open about who you are and what you are going to do with the personal data you collect. However, this is only one element of fairness. Providing a **privacy notice** does not by itself mean that your processing is necessarily fair.

You also need to consider the effect of your processing on the individuals concerned.

Therefore the main elements of fairness include:

- using information in a way that people would reasonably expect. This may involve undertaking preliminary endeavors to understand people's expectations about how their data will be used;
- assessing the impact of your processing. Will it have unjustified adverse effects on them? and;
- being transparent and ensuring that people know how their information will be used. This means providing **privacy notices** or making them available, using the most appropriate mechanisms. In a digital context this can include all the online platforms used to deliver services.

It is also important to recognise that the ways in which data is collected are changing. Traditionally, data was **collected** directly from individuals, for example when they filled in a form. Increasingly, organisations use data that has not been consciously provided by individuals in this way. It may be:

- **observed**, by tracking people online or by smart devices;
- **derived** from combining other data sets; or
- **inferred** by using algorithms to analyse a variety of data, such as social media, location data and records of purchases in order to profile people for example in terms of their credit risk, state of health or suitability for a job.

In these cases researchers are acquiring and processing personal data about individuals, and the requirement to be fair and transparent still arises. These new situations can make it more challenging to provide privacy information, and new approaches may be required.

A good way to approach these issues is to carry out a **Data Protection Impact Assessment (DPIA**). This is a methodology for assessing and mitigating the privacy risks in a project involving personal data. The University provides templates for DPIAs on the Data Protection pages on The Hub.

3.1.6 Further information – Good Practice

In addition to the required information that needs to go into a **privacy notice**, it is good practice for researchers to include the following in an information sheet:-

- The purpose of the research
- What is involved in participating in the research
- The benefits and risks in participating in the research
- Details of the research e.g. the funding source, sponsorship institution, name of project, contact details of researchers, and how to file a complaint

- The procedures for withdrawing from the research project
- The planned usage of the data during the research, dissemination, storage, publishing and archiving of the data
- The strategies for ensuring ethical use of the data
- The procedures for safeguarding personal data, maintaining confidentiality and anonymising data, particularly in relation to data archiving, sharing and reuse.

4. Lawful (Legal) Basis for Processing Personal Data

As stated earlier, research must have a valid lawful (legal) basis in order to process personal data and this basis should be stated in the **privacy notice** made available to potential participants.

There are six available lawful bases for processing. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the individual.

Most lawful bases require that processing is 'necessary'. You must determine your lawful basis before you begin processing, and it should be documented.

4.1 Lawful Basis (not special category data)

The lawful bases for processing are set out in Article 6 of the GDPR. **At least one of these must apply** whenever you process personal data (those in bold represent the conditions which commonly for research purposes). **Researchers must decide this ahead of collecting ANY personal data.**

Article 6

(a) Consent: the individual has given (or will give) clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law. (THIS WOULD BE RELIED UPON WHERE DATA ARE PROCESSED FOR RESEARCH PURPOSES BY A PUBLIC AUTHORITY SUCH AS UK UNIVERSITY, RESEACRH COUNCIL INSTITUTE OR AN NHS ORGANISATION).

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)PUBLIC AUTHORITIES INCLUDING UNIVERSITIES WILL NOT BE ABLE TO RELY UPON LEGITIMATE INTERESTS FOR RESEARCH ACTIVITIES AND OTHER PUBLIC TASKS.

4.1.1 Note on Consent

Researchers should be aware that most, if not all research will be suitably covered by identifying (e) Public Task as a legal basis for processing personal data. If (a) Consent is used as a legal basis for processing this gives additional rights to participants which in some research scenarios cannot easily be upheld. These rights can be found in section 4 but are only applicable if CONSENT is the legal basis for processing personal data.

The term consent has become ambiguous with the introduction of the GDPR. It is helpful if researchers consider splitting the meaning of consent into; **informed consent (as part of research ethics),** and **consent to process (GDPR) personal data**. This is discussed in more detail in section 3.

3.2 Special Category Data

If you are processing **special category data** you need to identify one of the above **Article 6** conditions for lawful basis as well as one of the following **Article 9** conditions for processing this type of data.

Special category personal data means personal data revealing: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership; and the processing of genetic data or biometric data for the purpose of uniquely identifying a natural person; data concerning health or data concerning sex life or sexual orientation.

Article 9

(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 referred to in paragraph 1 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 the conditions and safeguards referred to in paragraph 3

(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.

In particular, it should be noted that processing under Article 9 (j) will not meet the requirement that it is based on Member State law unless it satisfies the conditions set out in Part 1 of Schedule 1 of the Data Protection Bill 2017. This condition is met if the processing -

(a) is necessary for archiving purposes, scientific or historical research purposes or statistical purposes,
(b) is carried out in accordance with Article 89(1) of the GDPR (as supplemented by section 18), and
(c) is in the public interest.

4.1.2 What are Article 89 safeguards?

Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards. Those safeguards shall ensure that technical and organisational measures 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. Where those 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.

Please ensure you are familiar with the technical and organisational measures that the University requires researchers to follow, please see the Data Compliance webpages.

4. Consent to Process GDPR data

Researchers should note that the GDPR includes consent as a legal basis for processing personal data – this is **not the same as informed consent,** which is an ethical issue. GDPR defines consent 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..." **GDPR Article 4(11)**

If relying on consent as a legal basis then the following conditions must be adhered to:-

- Data subjects must be given the right to withdraw consent at any time
- Separate consents required for different processing activities
- Consent must be a positive indication of agreement to personal data being processed
- No longer rely on pre-ticked boxes or inactivity - does not constitute consent.
- You must be able to demonstrate that consent has been given
- The rights of participants and their data must be honoured

ICO Guidance on Consent – https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/consent/

Article 29 Working Party Guidance on Consent - http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

4.1 Explicit Consent to Process Special Category Data

Where you are relying on consent to process special categories data, consent must be explicit. The terms explicit refers to the way consent is expressed by the data subject. It means the data subject must give an express statement of consent for the processing of their special category data.

4.1.3 Consent in Practice

Researchers should:

- Inform participants about the purpose of the research
- Discuss what will happen with the contribution (including future archiving and sharing of data)
- Indicate the steps that will be taken to safeguard their anonymity and confidentiality
- Outline their right to withdraw from the research, and how to do this.

The GDPR recognises that it is not always possible to fully identify the purpose of personal data processing in research at the time of data collection, and, therefore, data subjects should be able to give their consent to certain areas of research (in keeping with recognised ethical standards for research) (recital 33)

4.1.4 Informed Consent. GDPR Consent and Research

Researchers should remember to separate **Informed Consent (Research Ethics)** and **Consent (as a legal basis to Process GDPR data)**. Informed Consent is frequently sought for participation in research and is an important part of the research process which serves many purposes. One reason that informed consent is sought may be to meet ethical

requirements, and to ensure that any disclosure of confidential data meets the requirements of the common law duty of confidence.

Again, it is important not to confuse informed consent e.g. an ethical or common law requirement, with the lawful basis for processing under GDPR legislation. **The lawful basis for processing personal data under data protection law may be something other than 'consent' with informed consent still sought for participation in the research to satisfy ethical requirements.**

> For example, an individual may be given a participant information sheet that requests if they will agree to participate in research (**consent to satisfy common law duty of confidence for example**), the information sheet will also describe that if they agree to participate, that the processing of their personal data will be necessary for the performance of a task carried out in the public interest or in the exercise of official authority (**the lawful basis under data protection legislation**). The requirements of data protection legislation apply alongside the requirements of other legal requirements when it comes to research for example such as common law duty of confidence: **both must be satisfied.**

If there are no alternative lawful bases available under the GDPR legislation and **consent** (Article 6(1(a)) is the only useful/applicable legal basis, researchers must understand what this means for research data. If using **consent** as the legal basis to process personal data and a participant withdraws their consent, research will no longer have a legal basis to hold onto any of their personal data that may already have been collected and this could potentially create a GDPR scenario which is very difficult for research to comply with.

Therefore, researchers must be mindful of the fact that when the **legal basis** for processing personal data is cited as **consent** - by default the data subject is legally given a number of rights including the right to withdraw consent and the right to data portability which might not be practicable or possible for research.

5. Data Subject Rights and Exemptions

The GDPR strengthens data subject rights: in relation to the right to be informed, the right of access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, and the right to object.

The GDPR also provides a parallel strengthening of 'research exemptions' and attaches some conditions to restrict the exercise of participant rights in the context of research processing. The restriction of data subject (participant) rights are only valid where 'appropriate safeguards' are in place (see earlier explanation of article 89 safeguards).

There is a distinction between research exemptions and conditions attached to the applicability of data subject (participant) rights introduced by the General Data Protection Regulation (GDPR) and those proposed by the Data Protection Act 2018.

Some restrictions, and conditions, are expressly provided by the GDPR. Namely, in relation to:

a) the right to erasure (Article 17)
b) the right to data portability (Article 20) and
c) the right to object (Article 21)

Further to this, the GDPR permits national law to introduce restrictions. Schedule 2, Part 6, Paragraph 27(2), of the Data Protection Act 2018 provides that, where personal data are being processed for research purposes, the following rights will **not** apply:

a) the right of access (Article 15)
b) the right to rectification (Article 16)
c) the right to restriction of processing (Article 18) and
d) the right to object (Article 21)

The application of an exemption is conditional and requires safeguards to be in place before an exemption can be valid.

'Safeguards' are measures to protect the rights and freedoms of individuals whose personal data you are processing. Appropriate safeguards **MUST** be in place before you can:

- lawfully process any type of personal data for research purposes – including sensitive ('special category') personal data concerning health ('Article 9'), and
- apply special exemptions under GDPR to enable research ('Article 89') e.g. being able to retain long term, medical records of individuals (which is not usually permitted)
-

The requirement for appropriate safeguards to apply to personal data processed for research purposes is not new. Section 33 of the Data Protection Act 1998 specified 'relevant conditions' that had to be satisfied in order for specific exemptions to be available where data was being processed for research purposes.

5.1 Minimum Safeguards

A. Section 19 Safeguards

Section 19 (parts 2 and 3)of the Data Protection Act 2018 makes clear that the requirement for appropriate safeguards for the rights and freedoms for the data subject established by the GDPR cannot be satisfied if the processing is:

(2) is likely to cause substantial damage or substantial distress to a data subject.
(3) 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.

B. Technical and Organisational Measures

Article 89(1) of the GDPR makes clear that to satisfy the requirement for appropriate safeguards, an organisation must ensure, that technical and organisational measures are in place. This applies to processing of all personal data. In particular, the principle of data minimisation (i.e. using only the absolute minimum of personal data required for a purpose) should be respected. Minimisation requires at least:

> (a) Personal data is pseudonymised where compatible with achievement of the research purpose, and
> (b) Where research purposes can be fulfilled by further processing with anonymised data, then identifiable data is not used

C. Schedule 1 safeguards: applicable only to special categories of data

To satisfy the conditions established by Part 1 of Schedule 1 of the Data Protection Act, where processing is in reliance of article 9(2)(j) – and it is necessary for research purposes to process special categories of data including health and other data – then another safeguard applies: processing must be "**in the public interest**".

D. Data Protection Act 2018

In addition to the appropriate safeguards listed above, the Data Protection Act 2018 proposes that one may appropriately restrict a data subject's rights in the research context only where:

> (a) the application of the data subjects rights would prevent or seriously impair the achievement of the research purpose.

5.2 Exemptions for Research (where consent has been used as a lawful basis for processing)

Exemption	Description	Mitigation
Rights of access by the data subject (Article 15)	Data Protection legislation provides an individual data subject with the right to access his or her personal data. The right of access extends to include not only a right to a copy of the personal data undergoing processing but also to access to information about the purposes of processing, the categories of data processed, the recipients – particularly those in third countries or international organisations, the envisaged storage period, existence of relevant data subject rights, right to lodge a complaint with the ICO, the source of the data, specific information about any automated processing, and, where data are transferred to a third country or international organisation, information about the appropriate safeguards to be applied.	The right of access does not apply when data are processed for research purposes where: 1. the requirement for 'appropriate safeguards A-D' is met; and either, 2. the results of the research or any resulting statistics are not made available in a form which identifies the data subject; or, 3. in the opinion of an appropriate health professional, disclosure to the data subject is likely to cause serious harm.
Exemption - Right to rectification (Article 16)	Data Protection legislation provides individual data subjects with the right to obtain from the controller, without undue delay, the rectification of inaccurate personal data concerning him or her. This can include having incomplete personal data completed, including by means of providing a supplementary statement.	This right to rectification does not apply where data are processed for research purposes and the requirement for 'appropriate safeguards A-D' is met.
Exemption - Right to erasure ('Right to be forgotten') (Article 17)	Data Protection legislation provides individual data subjects with the right to request erasure of personal data in specific circumstances. (This includes pseudonymised data as defined by the GDPR.)	This right to erasure does not apply where data are processed for research purposes and the requirement for 'appropriate safeguards A-D' is met. **Example:** Erasing data when a database has been locked for analysis would seriously impair achievement of the purposes of a research activity (as would rectification when the research is based on a snapshot of time). The right to erase need not be applied where erasure would prevent or seriously impair achievement of the research purpose and other appropriate safeguards are met.

Exemption - Right to Erasure and Consent	The significance of the research restriction (on the right to erasure) is reduced when consent is the lawful basis for processing under data protection law. If consent is the lawful basis for processing, then a withdrawal of consent will have the result that data needs to be erased even if this is likely to render impossible or seriously impair the achievement of the objectives of that processing. This is because there will no longer be a lawful basis to hold the data.	This underlines the importance of ensuring that, when specifying the legal basis upon which data is processed, consent is only specified as the relevant legal basis where there are no more suitable alternatives.
Exemption - Right to restriction of processing (Article 18)	Data Protection legislation provides individual data subjects with the right to restrict the processing of data by the controller in specific circumstances. For example, if a data subject contests the accuracy of data, then he or she has the right to obtain from the controller a restriction of processing for a period to enable the Controller to verify the accuracy.	This right to restrict processing does not apply where data are processed for research purposes and the requirement for 'appropriate safeguards A-D' is met.
Exemption - Right to data portability (Article 20)	Data Protection legislation provides individual data subjects with the right to data portability. This right facilitates a data subject's ability to move, copy or transmit personal data easily from one IT environment to another.	The right only applies where the processing is carried out by automated means (i.e. electronically) and where the data were provided to the controller by the data subject and also where processing is on the basis of either consent or contract.There is no obligation upon a controller to answer a data portability request where the lawful basis of processing is something other than **consent** or **contract**. So, the right to data portability is not applicable to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller.
Exemption - Right to object (Article 21)	Data Protection legislation provides individual data subjects with the right to object to the processing of personal data about them. An objection may prevent processing even where consent is not the lawful basis for processing (under Article 6 or Article 9 GDPR).	The right to object does not apply where data are processed for research purposes if: i) the requirement for appropriate safeguards A-D is met, and ii) the processing is necessary for a task carried out in the public interest.
Advice from the Data Protection Officer should be sought by a researcher before responding to any external or internal query, request, or exercise of a data subject's rights		

6. Data Transfers Outside of the EU

There are three main routes to lawfully transfer personal data outside of the EU:

1. A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection.

2. In the absence of an 'adequacy decision' from point 1, personal data can be transferred to a third country where the controller or the processor has provided appropriate safeguards. Appropriate safeguards which do not require specific authorisation from the ICO include:

    - a legally binding agreement between public authorities or bodies;
    - binding corporate rules (agreements governing transfers made between organisations within in a corporate group);
    - standard data protection clauses in the form of template transfer clauses adopted by the Commission;
    - standard data protection clauses in the form of template transfer clauses adopted by a supervisory authority and approved by the Commission;
    - compliance with an approved code of conduct approved by a supervisory authority;
    - certification under an approved certification mechanism as provided for in the GDPR;
    - contractual clauses agreed authorised by the competent supervisory authority; or
    - provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority.

3. In the absence of either of the aforementioned routes, there are derogations for specific situations in Article 49 which may permit the transfer for example where the data subject has consented to the purpose of the transfer after having been informed of the possible risks of such a transfer due to the absence of an adequacy decision and appropriate safeguards (Note, consent is not an option when a public authority is exercising public powers)

When choosing where to store personal data, it is important to consider how best to protect that personal data and whether it is appropriate to be transferred or stored outside the EU.

Personal data should be minimised, and pseudonymised or anonymised - as appropriate – and technical measures such as encryption should be utilised to help protect that data.

Pseudonymisation is defined as '**the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person' (Article 4(5))**

7. High Risk Processing (special category data)

The introduction of the new accountability principle under the GDPR requires organisations to understand the risks they create, to mitigate them and to be able to demonstrate that they comply. Some measures that were previously recommended as being good practice are now legally required – these include **data protection by design** and **privacy impact assessments.**

7.1 Data protection by design

When embarking on a new research project, organisations will need to show that they have considered and integrated data protection into their processing activities from the initial stages of the design process. It is a mandatory requirement to ensure that privacy and data protection are key considerations in the early stages of any project, and then throughout its lifecycle.

Ways to support the evidencing of data protection by design would include:

- Documenting all strategies and controls that have already been deployed and that are applied
- Involving the organisation's Data Protection Officer to help rank and order risks for mitigation.
- Ensuring security / system providers demonstrate that they are compliant.
- Applying the ICOs current guidance on Privacy Impact Assessment or Data Protection Impact Assessment (DPIA) through all parts of the organisation.
- Creating privacy impact assessment documentation and processes.

Taking a **privacy by design** approach is an essential tool in minimising privacy risks and building trust. Designing projects, processes, products or systems with privacy in mind at the outset can lead to benefits which include:

- Potential problems are identified at an early stage, when addressing them will often be simpler and less costly.
- Increased awareness of privacy and data protection across an organisation.
- Organisations are more likely to meet their legal obligations and less likely to breach the Data Protection Act.
- Actions are less likely to be privacy intrusive and have a negative impact on individuals.

7.2 Data Protection Impact Assessments (DPIA)

A tool for organisations to use to identify effective ways to comply with the GDPR obligations. The Information Commissioner's Office (ICO) will expect to see data protection by design demonstrated by use of a Privacy Impact Assessment or Data Protection Impact Assessment (DPIA). A privacy impact assessment is mandatory when:

- Using new technology – this can trigger the need to carry out a privacy impact assessment as it can involve novel forms of data collection and usage, possible with high risk to individual's rights and freedoms.
- Where the processing is likely to result in a high risk to the rights and freedoms of individuals.

High risk processing will include:

→ Evaluation or scoring, including profiling and predicting, especially from 'aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements'. An example would be where an organisation builds behavioural or marketing profiles based on usage or navigation of its website.
→ Automated-decision making with legal or similar significant effect. Examples of this would be where processing may lead to the exclusion or discrimination against individuals.
→ Systematic monitoring – processing used to observe, monitor or control data subjects e.g. CCTV
→ Special categories of data or sensitive personal data – e.g. patient medical records in a hospital or a personal data relating to criminal convictions. This refers mainly to processing sensitive personal data on a large scale where there is increased possible risk to rights and freedoms of individuals. An organisation organising a corporate event collecting data on guest allergies is processing sensitive personal data however would not need to perform a PIA.
→ Data processed on a large scale – this would depend on number of data subjects, volume of data, duration of processing activity and geographical extent of the processing activity.
→ Data concerning vulnerable data subjects.
→ Data transfer across borders outside the European Union.

Please liaise with the Data Protection Officer if you are not sure if your project is high risk and requires a Data Protection Impact Assessment

7.3 Contracts and Third Party Data Processing

The GDPR imposes a high duty of care upon controllers in selecting their personal data processing service providers, which will require procurement processes and requests for tender documents to be regularly assessed. Contracts must be implemented with these service providers which include a range of information (e.g. the data processed and the duration for processing) and obligations (e.g. assistance where a security breach occurs, appropriate technical and organisational measures taken and audit assistance obligations). Likewise, this requirement applies where a service provider hires a sub-processor. Examples of organisations which provide services to other businesses as data processors are companies providing cloud storage, data collection services, IT services, HR functions, marketing services and payroll services.

Under the GDPR, the following requirements will apply to you if you are a data controller:

- Before appointing a data processor, you will need to carry out appropriate due diligence and satisfy yourself that the data processor will be able to meet the requirements of the GDPR.
- You will need to enter into a written contract with the data processor.
- Your contract with the data processor will need to contain various contract terms, which are specified in the GDPR.

The above requirements will apply with immediate effect from **25th May 2018** to both new processing contracts and your existing contracts with data processors. The University will therefore need to:

- Review and amend any existing contracts with data processors that will still be in force when the GDPR becomes effective in May 2018, to ensure that the GDPR requirements are incorporated.
- Ensure that any future agreements with data processors meet the new requirements.

It is also important to note that, under the GDPR, data processors (as well as data controllers) will be subject to certain statutory obligations. This is a significant change, as it means that enforcement action can be taken by regulatory bodies (such as the ICO) against data processors, that data processors can be fined for breach of the GDPR and that they can be sued for compensation by the individuals whose data they process.

A template Data Processing Agreement is available on the Data Protection pages on The Hub.

8. Contacts

All queries should be relayed to the Data Protection Officer of the University

Mr Rhys Davies Rhys.davies@southwales.ac.uk

OR

the Research Governance Officer

Mr Jon Sinfield Jonathan.sinfield@southwales.ac.uk

Appendix 1 – Template Privacy Notice

Privacy Notice

The University of South Wales is the data controller with regard to this personal information, and it is committed to protecting the rights of individuals in line with the Data Protection Act 1998 (DPA) and the new General Data Protection Regulation (GDPR). The University of South Wales has a Data Protection Officer who can be contacted through dataprotection@southwales.ac.uk

What information we collect?

The University collects the following information:

Outline what types of personal data are being processed. It is important to be aware of which type of data is being processed as this may alter the legal basis for processing (referred to in the next section).

The GDPR defines **personal data** as the following:

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;

Personal data relating to Employee/student, can include: name, job title, date of birth,

passport data, home address, home telephone number, private email address, emergency contact, staff number etc.

'**Special categories**' of personal data relate to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

Special category data relating to employee/student can include: racial and ethnic origin, religion, health records etc.

Why we collect this information?

USW has to collect personal data to satisfy a number of requirements:

The purposes of the processing should be outlined. Examples provided below:

- administering finance (e.g. fees, scholarships and bursaries)
- providing student support services
- providing library, IT and information services
- managing student accommodation
- monitoring equal opportunities
- carrying out research and statistical analysis
- providing operational information
- promoting our services
- safeguarding and promoting the welfare of students
- ensuring student's safety and security
- preventing and detecting crime.
- will the data be used to make automated decisions?

What is our legal basis for processing?

In processing the personal data of staff the University relies upon the following legal basis as appropriate:

For processing to be lawful under the GDPR, it would be necessary to identify a lawful basis before personal data is processed. It is important that the lawful basis is determined and this is documented.

Where personal data is processed then a condition under Article 6 must be satisfied. If special category data (formerly known as sensitive data) then it is necessary for an article 9 category to be satisfied.

Article 6 - Personal Data	**Article 9 - Special Categories**
The data subject has given ***consent*** to the processing *	The data subject has given ***explicit consent*** to the processing
Processing is necessary for the performance of a ***contract*** with the data subject	Processing is necessary for the purposes of carrying out the obligations of the controller or of the data subject in the field of ***employment***
Processing is necessary for compliance with a ***legal obligation***	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
Processing is necessary in order to protect the ***vital interests*** of the data subject or of another natural person	Processing is carried out in the course of its legitimate activities by a foundation, association or any other ***not-for-profit*** body with a political, philosophical, religious or trade union aim.
Processing is necessary for the performance of a task carried out in the ***public interest***	Processing relates to personal data which are made ***public*** by the data subject

Processing is necessary for the purposes of the ***legitimate interests*** pursued by the controller or by a third party. This condition can only be used by the University if processing does not fall within our core function which is providing education and conducting research**	Processing is necessary for the establishment, exercise or defence of ***legal claims*** or whenever courts are acting in their judicial capacity
	Processing is necessary for reasons of ***substantial public interest***
	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
	Processing is necessary for reasons of public interest in the area of ***public health***
	Processing is necessary for ***archiving purposes*** in the public interest, scientific or historical research purposes or statistical purposes

***** If researchers are using CONSENT as the LEGAL BASIS for processing personal information:

It is worth noting that rules around consent are much stricter under GDPR. Consent means offering individuals genuine choice and control and requires a positive opt-in. Pre-ticked boxes and any other methods of consent by default are not lawful.

The GDPR gives individuals a specific right to withdraw consent. It is necessary to tell individuals around their right to withdraw consent and offer them easy ways to withdraw consent at any time. Consider the implications for your research data and if there will be limits in allowing personal data to be withdrawn, such as after data anonymisation.

OR

** In order to rely on the 'legitimate interests' condition certain requirements must be met.

The first requirement is that there must be a necessity to process the information for the purposes of the University's legitimate interests or for those of a third party to whom the information will be disclosed.

The second requirement, once the first has been established, is that these interests must be balanced against the interests of the individual(s) concerned. The "legitimate interests" condition will not be met if the processing is unwarranted because of its prejudicial effect on the rights and freedoms, or legitimate interests, of the individual. The legitimate interests do not need to be in harmony with those of the

individual for the condition to be met. However, where there is a serious mismatch between competing interests, the individual's legitimate interests will come first.

Who are the recipients or categories of recipients?

Recipient means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.

Where necessary personal information will be shared internally within the faculties and departments across the University. Such sharing will be subject to confidentiality protocols and access restrictions.

This section outlines the major organisations to which we may disclose data:

Personal data may also be disclosed when legally required or where there is a legitimate interest, either for the University or the data subject, taking into account any prejudice or harm that may be caused to the data subject.

The University may also use third party companies as data processors to carry out certain administrative functions on behalf of the University. If so, a written contract will be put in place to ensure that any personal data disclosed will be held in accordance with the data protection laws.

Transfers to third countries and the safeguards in place

Here it is necessary to specify if the data will be transferred outside of the EU.

Retention of data

All data held about USW activities and all personal data will stored securely and appropriately in line with the University's Retention Schedule

This Schedule is reviewed periodically and it serves to determine how long certain information will be retained.

Security of data

Data Protection legislation requires us to keep your information secure. This means that your confidentiality will be respected, and all appropriate measures will be taken to prevent unauthorised access and disclosure. Only members of staff who need access to relevant parts or all of your information will be authorised to do so. Information about you in electronic form will be subject to password and other security restrictions, while paper files will be stored in secure areas with controlled access.

Some processing may be undertaken on the University's behalf by an organisation contracted for that purpose. Organisations processing personal data on the

University's behalf will be bound by an obligation to process personal data in accordance with Data Protection legislation.

Your rights

You have a right to access your personal information, to object to the processing of your personal information, to rectify, to erase, to restrict and to port your personal information.

Please visit the University Data Protection webpages for further information in relation to your rights.

Any requests or objections should be made in writing to the University Data Protection Officer:-

University Secretary's Office,
University of South Wales
Pontypridd,

CF37 1DL

Email: dataprotection@southwales.ac.uk

If you are unhappy with the way in which your personal data has been processed you may in the first instance contact the University Data Protection Officer using the contact details above.

If you remain dissatisfied then you have the right to apply directly to the Information Commissioner for a decision. The Information Commissioner can be contacted at:

Information Commissioner's Office,
Wycliffe House,
Water Lane,
Wilmslow,
Cheshire,
SK9 5AF

www.ico.org.uk

Version Control:

Drafted: 10/09/2018	Author: Jon Sinfield / Rhys Davies	To be reviewed: 10/09/2019