DE MONTFORT UNIVERSITY LEICESTER

Research Directorate

UK GENERAL DATA PROTECTION REGULATION (GDPR) GUIDANCE FOR RESEARCHERS

Created and Modified:	21 January 2021
Last Updated	19 April 2021
Author:	Susie Fowler
Originating Department:	Research Services Directorate
Approved by:	DMU Research Ethics Committee DMU Research & Innovation Committee

DE MONTFORT UNIVERSITY

UK GDPR GUIDANCE FOR RESEARCHERS

Contents

1 Introduction

1.1 What is UK GDPR?

1.1.1 The EU General Data Protection Regulation (EU-GDPR) is legislation that was introduced on 25 May 2018, to protect the rights and freedoms of EU Citizens with respect to their Personal Identifiable Information and defined who and how their data could be used and retained, thus requiring all organisations that process data of EU citizens, irrespective of whether they are based in the Union or not, to be compliant with the regulation. It also applied to all organisations within the Union, even if data processing takes place outside of the Union.

1.1.2 Following the UK's exit from the EU, the EU-GDPR ceased to apply in the UK, other than for EU citizens. However, the GDPR has been retained in UK law (essentially mirroring the EU-GDPR) and will continue to be read alongside the Date Protection Act 2018, with technical amendments to ensure it can function in UK law.

1.1.2 Although the GDPR was not written specifically for research activities, it is important that researchers understand the implications of the GDPR in relation to their role, their research and the data being collected and processed.

1.1.3 The GDPR protects the fundamental rights and freedoms of people (data subjects) and in particular their right to the protection of their own personal data, how that data is processed and rules relating to the free movement of personal data.

1.1.4 For the GDPR to apply, you **must be** processing personal data (see definition in 1.2.1.1 below).

1.1.5 The GDPR recognizes new **privacy rights for data subjects**, which aim to give individuals more control over their data (see **Section 7 – GDPR Safeguards)**. It is important to understand these rights to ensure you are GDPR compliant.

1.2 Useful Definitions

1.2.1 Below are some of the most important and common definitions that relate to the GDPR. This document will expand on issues such as personal data in later sections:

1.2.1.1 **Personal data** — this is any information that relates to an individual that will allow the individual to be directly or indirectly identified. This might include, for example, name, date of birth, an ID number, or location information.

1.2.1.2 **Data processing** — any action performed on data, whether automated or manual. Examples include collecting, recording, organizing, structuring, storing, using, and erasing.

1.2.1.3 **Data subject** — the person whose data is being processed (e.g. research participants).

1.2.1.4 **Regulator** – the body that provides guidance for compliance with the new legislation and is the Information Commissioner's Office (ICO).

1.2.1.5 **Data controller** — the organisation that decides why and how personal data will be processed.

1.2.1.6 **DMU is the data controller --** this means that DMU (alone or jointly with other controllers) determines the purpose and the means of processing personal data. The means of processing includes responsibility for protecting the personal information processed. Where DMU processes data on behalf of another controller, DMU are a processor and not the controller. DMU as a controller may use other organisations to process data on our behalf.

1.2.1.7 **Data processor** — a third party that processes personal data on behalf of a data controller. The data controller must issue instructions to the data processor on the processing of personal data.

2 Key Areas for Consideration

2.1 When designing and planning your research project, it is important to understand how GDPR may affect your work. The introduction of GDPR has meant some significant changes for anyone using identifiable data in their research.

2.2 The GDPR is only concerned with information that can be used to **identify living people**, so if you are intending to conduct research using live data subjects, you should consider the following questions:

2.2.1 Do I have a lawful basis for processing the data (see Section 4 for what constitutes 'lawful bases')?
2.2.2 Does the research involve handling personal information, including (but not limited to) pseudonymised data, consent forms (for studies where data is not otherwise stored)?
2.2.3 What type of personal information will I be processing?
2.2.4 Will it be anonymised?
2.2.5 Is it classed as 'Special Category Data'? (see Section 6.5 on special category data)
2.2.6 Does the participant information sheet and consent form include sufficient information to meet the GDPR requirements of transparency?
2.2.7 How am I going to protect my participants' information?
2.2.8 How long am I allowed to keep the data?
2.2.9 Is there any possibility that we may want to use the personal data for purposes other than that the participants are told of?

2.3 These guidelines aim to highlight some of the key areas that you need to be aware of when planning and conducting research that involves the processing of personal data.

2.4 *Never* assume that ways you were working previously are now GDPR compliant. It is important to review, re-assess and make sure that everything you do is GDPR compliant.

3 General Principles

3.1 There are seven key principles laid down under GDPR Article 5 which should be taken into consideration when planning a research project and should shape your approach to processing personal data.

3.2 The principles[1] require that personal data shall be:

3.2.1 processed lawfully, fairly and in a transparent manner;
3.2.2 only collected for specified, explicit and legitimate purposes (**purpose limitation**);
3.2.3 adequate, relevant and limited to what is necessary (**data minimisation**);
3.2.4 accurate, up-to-date, with inaccuracies erased or rectified without delay (**accuracy**);
3.2.5 kept for no longer than is necessary – depending on the nature of the processing (**storage limitation**);
3.2.6 processed in a manner that ensures appropriate security of the personal data (**confidentiality and integrity**);
3.2.7 accountability.

[1] For a full explanation of the seven principles, please refer to the guidance available on the **Information Commissioner's Office** website.

4 Lawful Bases for Processing

4.1 Before exploring lawful bases for data processing, it is important to understand what constitutes processing.

4.2 As defined in Section 1.2, processing constitutes **any** action performed on data, whether automated or manual, i.e. collecting, recording, organizing, structuring, storing, using, erasing etc. For example: if there is a conversation between two people where an opinion might be expressed in relation to someone's details, but the conversation is not recorded, the data is **not** being processed. However, if some work had been required beforehand to obtain the information being discussed, and the conversation was recorded and later written up, this *would* be classed as processing. If you are in any doubt, you should contact your GDPR lead or the Information Governance Team (dataprotection@dmu.ac.uk)

4.3 The requirement to have a **lawful basis** in order to process personal data is not new. It replaces the requirement to satisfy one of the 'conditions for processing' previously stipulated under the Data Protection Act 1998. However, the GDPR places more emphasis on being **accountable** for and **transparent** about lawful bases for processing.

4.4 GDPR Article 6 identifies that organisations must meet all relevant legal requirements to collect and process personal data – referred to as a 'lawful basis'. There are six lawful bases that can be applied. The one you chose will depend on your purpose for processing the data and your relationship with the individual. You may only use one lawful basis for any specified processing.

4.4.1 Many of the lawful bases for processing depend on the processing being "necessary". This does not mean that processing always has to be essential. However, it must be a targeted and proportionate way of achieving the purpose. **NB:** "Most lawful bases require that processing is 'necessary'. If you can reasonably achieve the same purpose without processing, you won't have a lawful basis" (BPS, 2018). Lawful bases include:

4.4.1.1 **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.

4.4.1.2 **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.

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

4.4.1.4 **Vital interests:** the processing is necessary to protect someone's life.

4.4.1.5 **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.

4.4.1.6 **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.)

4.4.2 For full relevant provisions in Article 6 see Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) (legislation.gov.uk)

You should determine your lawful basis **before** you begin processing your data and document this accordingly. However, the most likely basis for research carried out in universities is '**public task'** as explained by the ICO:

4.4.2.1 A university that wants to process personal data may consider a variety of lawful bases depending on what it wants to do with the data. Universities are likely to be classified as public authorities, so the public task basis is likely to apply to much of their processing, depending on the detail of their constitutions and legal powers. If the processing is separate from their tasks as a public authority (for example, for commercially funded research), then the university may instead wish to consider whether consent or legitimate interests are appropriate in the particular circumstances, considering the factors set out below.

4.4.2.1.1 For example, a University might rely on a public task for processing personal data for teaching and research purposes, but a mixture of legitimate interests and consent for alumni relations and fundraising purposes. The university however needs to consider its basis carefully – it is the controller's responsibility to be able to demonstrate which one lawful basis applies to the particular processing purpose.

4.4.3 UK Research & Innovation (UKRI) advises 'organisations can demonstrate they meet the requirements to use this lawful basis by reference to their legal constitutions, or because they are operating under a relevant statute that specifies research as one of the purposes of the organisation'.

4.4.4 By using 'public task'[2] as the lawful basis for processing data, research participants can be reassured that their interests are protected and that:

- The organisation/ institution is credible
- Personal data is necessary
- Personal data will only be used to support legitimate research that is considered to be in the public interest.

4.4.5 Information about the lawful basis (or bases, if more than one applies) is set out in the DMU online privacy notice.

4.4.6 Under the transparency provisions of the GDPR, the information you need to give people includes: your intended purposes for processing the personal data; and the lawful basis for the processing. This applies whether you collect the personal data directly from the individual or you collect their data from another source. This information should be included as part of your participant information sheet.

4.4.7 If you are processing 'Special Category Data', you must identify the lawful basis AND satisfy an additional processing condition (see Section 6.5). Please contact your GDPR Lead or the Information Governance Team for any advice.

4.5 In relation to accountability, the following points need to be considered:

4.5.1 ICO guidance in relation to understanding accountability advises that you should be able to demonstrate that you are complying with the GDPR, by adhering to appropriate policies and processes put in place by DMU (your Data Controller). This means that you need to be able to show that you have properly considered which lawful basis applies to each processing purpose and can justify your decision. You need therefore to keep a record of which basis you are relying on for each processing purpose, and a justification for why you believe it applies. **Much of this will be detailed in DMU's Privacy Notice, though it is still your responsibility as a researcher to show that you can demonstrate which lawful basis applies to the particular processing purpose you intend to use**. This can be included in your research proposal. Data Protection Impact

[2] The full guidance in relation to public task is available on the **Information Commissioner's Office website.**

Assessments are the most likely method of demonstrating accountability, and the ICO stipulates these must be completed where there is a high risk to the rights and freedoms of individuals.

4.5.2 If you are processing **special category data**, you need to identify both a lawful basis for processing and a special category condition for processing in compliance with Article 9 of the GDPR. In order to demonstrate both compliance and accountability, you should document both your lawful basis for processing **and** your special category condition.

4.6 Transparency

4.6.1 Under the transparency provisions of the GDPR, the information you need to give people includes: your intended purposes for processing the personal data, and the lawful basis for the processing, and should be included as part of your participant information sheet. You should also make them aware of their rights. This applies whether you collect the personal data directly from the individual or you collect their data from another source. You should always provide a link to the DMU Data Protection pages on any information provided, https://www.dmu.ac.uk/policies/data-protection/data-protection.aspx.

5 Consent to Process Personal Data versus Ethical Consent

5.1 When we refer to consent as a lawful basis for processing personal data, this is not the same as an individual's ethically informed consent to taking part in a research project.

5.2 When an individual provides informed consent as part of the ethical considerations of a research project, they are confirming that they have received and understood detailed information about the project, its purpose and how their data with be used. They have made a voluntary and informed decision to take part in the research, based on that information.

5.3 Consent as a lawful basis to process personal data under the GDPR means giving people genuine choice and control over how you use their data. If the individual has no real choice, consent is not freely given and it will be invalid.

5.4 Even if individuals have consented to participate in the research, you will usually find that a different lawful basis (as well as a different special category data condition if this type of data is used) is more appropriate in the circumstances. People must be able to refuse consent without detriment, and must be able to withdraw consent easily at any time. Full guidance on GDPR consent requirements can be accessed via The Information Commissioner's Office. If you are relying on Consent as a lawful basis, you will be required to delete personal data if consent is withdrawn at any time.

6 Types of Data

6.1 Personal Data

6.1.1 Personal data is defined in law as "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" (GDPR Article 4(1)).

6.1.2 In order to ascertain if the GDPR applies to your processing, it is imperative to understand if the data is classed as personal data. The ICO guidance is thus:

6.1.2.1 If it is possible to identify an individual directly from the information you are processing, then that information may be personal data.

6.1.2.2 If you cannot directly identify an individual from that information, then you need to consider whether the individual is still identifiable. You should take into account the information you are processing together with all the means reasonably likely to be used by either you or any other person to identify that individual (What is personal data?).

6.1.2.3 **If personal data can be truly anonymised then the anonymised data is not subject to the GDPR**. As such, it is important to understand what constitutes personal data in order to understand if the data has been anonymised.

6.1.2.4 Information about a deceased person does not constitute personal data and therefore is not subject to the GDPR although other legislation will need to be considered.

6.1.2.5 Information about companies or public authorities is not personal data. However, information about individuals acting as sole traders, employees, partners and company directors where they are individually identifiable and the information relates to them as an individual may constitute personal data.

6.2 Personal Data Identifiers

6.2.1 A person can be identified through a single identifier, or a combination of identifiers. The GDPR provides the following as examples of identifiers:

- Name
- Identification number
- Location data and
- An online identifier (including IP address and cookies)

6.2.2 Other identifiers may include:

- Physical and psychological factors
- Biometrics
- Genetic
- Mental
- Economic
- Cultural or social identity

6.2.2.1 In order to decide if data is classed as personal, a good guide is to ask 'Can I identify an individual directly from this information, or a combination of information available to my organisation?'

6.2.2.2 ICO guidance is as follows:

- If, by looking solely at the information you are processing you can distinguish an individual from other individuals, that individual will be identified (or identifiable) and so **this would constitute personal data**.
- You don't have to know someone's name for them to be directly identifiable; a combination of other identifiers may be sufficient to identify the individual.
- If an individual is directly identifiable from the information, **this may constitute personal data.**
- When considering whether individuals can be identified, you may have to assess the means that could be used by an interested and sufficiently determined person.

6.2.2.3 NB: Anyone handling such personal data, as described, is required to identify which lawful basis permits the data's usage.

6.3 Anonymised Data

6.3.1 Where steps have been taken to reduce how readily individuals can be identified by their personal data, this can affect how much the GDPR impacts the data. **The GDPR does not apply if your research deals only with FULLY ANONYMISED DATA (i.e. there is no way of linking it back to the individual it relates to).**

6.3.2 Recital 26 of the GDPR states that:

"The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes."

6.3.3 As such FULLY anonymised data is not covered by the GDPR and can therefore be a method of limiting your risk. **Anonymising data wherever possible is therefore encouraged.**

6.3.4 **NB:** We must take note that information which DOES NOT contain names, or similar unique identifiers, may STILL NOT be sufficiently anonymous. E.g., biographical details may be sufficient for some individuals to be identifiable within their peer group.

6.4 Pseudonymised Data

6.4.1 Pseudonymisation is a security measure and not a form of anonymisation. It is a technique that replaces or removes information in a data set that identifies an individual. Where the controller (DMU) holds the key/additional data which would allow identification of individuals, this data which we hold is still identifiable and so is not considered to be anonymised, thus GDPR **would** be applicable. For example, if names were removed from a dataset and replaced with alphanumerical identifiers (e.g. *SubjectA01, Subject A02* etc.), but a separate file was retained linking each name with its number, this would permit the re-association of the data with the specific individuals. Hence, pseudonymisation reduces, but does not remove risk for individuals from data protection incidents.

6.4.2 Where a key exists that can reidentify individuals, the data is only ever pseudonymised. The data may be more secure, but if there is still a way to identify individuals from a key, the data would not have been truly anonymised.

6.5 Special Category Data

6.5.1 Under the Data Protection Act 1998, the term **sensitive personal data** was used. This is now defined as **Special Category Data**. This data requires more protection as it is considered to be more 'sensitive,' and could create more significant risks to a person's fundamental rights and freedoms. Under the GDPR, genetic and some biometric data is now included in the scope of this definition. It does not include information relating to criminal offences and convictions; this is subject to separate safeguards as set out in Article 10 and explained further in the next section.

6.5.2 Special Category Data *can* be processed for research purposes as long as it is:

- Necessary for archiving proposes, scientific or historical research purposes or statistical purposes;
- Subject to appropriate safeguards; and ➢ In the public interest.

6.5.3 Special Category Data includes:

- Race;
- Ethnic origin;
- Political or philosophical opinions;
- Religion;
- Trade union membership;
- Genetics;
- Biometrics (where used for ID purposes);
- Health;
- Sex life; or
- Sexual orientation.

6.5.4 You must still satisfy the requirement to process special category data in line with Article 6 (as with any other personal data), however, you can only process special category data if you can *additionally* meet one of the specific conditions in Article 9 of the GDPR. Determine your condition for processing special category data before you begin and document this clearly.

6.5.5 You must do a **Data Protection Impact Assessment** (DPIA) for any type of processing that is likely to result in a high risk to the rights and freedoms of natural persons This means that you are more likely to need a DPIA for processing special category data. For further information, please see guidance in Section 9.

6.6 Conditions for Processing Special Category Data

6.6.1 The conditions are listed in Article 9(2) of the GDPR thus:

6.6.1.1 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;

6.6.1.2 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;

6.6.1.3 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;

6.6.1.4 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;

6.6.1.5 processing relates to personal data which are manifestly made public by the data subject;

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

6.6.1.7 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;

6.6.1.8 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;

6.6.1.9 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;

6.6.1.10 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.

6.6.2 It should be noted that in some of the above cases, reference to specific sections of the Data Protection Act 2018 will be required, in particular but not exclusively condition G. If in doubt please contact the Information Governance Team.

6.6.3 Non-commercial research conducted at DMU is done in the public interest, therefore, where our research involves special category data, we will rely on one of the public interest lawful bases to process special category data, in addition to the lawful basis of 'public task' for general processing. (Commercial research would be classed differently and will likely require a different legal basis for processing. Legitimate Interest may be more appropriate. The Information Governance Team can advise the best legal basis in these instances[3]).

6.7 Criminal Offence Data

6.7.1 What is criminal offence data? This covers a wide range of information about: criminal activity; allegations; investigations and proceedings.

6.7.2 It includes not just data which is obviously about a specific criminal conviction or trial, but also any other personal data relating to criminal convictions and offences, including: unproven allegations; information relating to the absence of convictions and personal data of victims and witnesses of crimes.

6.7.3 It also covers a wide range of related security measures, including persona; data about penalties; conditions or restrictions placed on an individual as part of the criminal justice process; or civil measures which may lead to a criminal penalty if not adhered to.

6.7.4 The GDPR rules for sensitive (special category) data do not apply to information about criminal allegations, proceedings or convictions. To process personal data about criminal convictions or offences, you must have both a lawful basis under Article 6 and either legal authority or official authority for the processing under Article 10.

[3] For more detailed guidance see Special category data | ICO

6.7.5 Article 10 applies to personal data relating to criminal convictions and offences, or related security measures. Criminal offence data includes the type of data about criminal allegations, proceedings or convictions that would have been sensitive personal data under the 1998 Act, but also extends to personal data linked to related security measures.

6.7.6 Article 10 states: "Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority."

6.7.7 This means you must either:

- process the data in an official capacity; or
- meet a specific condition in Schedule 1 of the Data Protection Act 2018, and comply with the additional safeguards set out in that Act

6.7.8 Even if you have a condition, as per Article 9 (2) (section 6.6.1 above) for processing offence data, you can only keep a comprehensive register of criminal convictions *if* you are doing so in an official capacity. You should always seek advice from the Information Governance Team if you are considering processing criminal offence data[4].

6.7.9 You must complete a **Data Protection Impact Assessment** (DPIA) for any type of processing which is likely to be high risk. You must therefore be aware of the risks of processing criminal offence data. See Section 10 for full details regarding DPIAs.

6.7.10 When intending to process criminal data, you should always contact the Information Governance Team. This is a more specialised area and advice should always be taken. Both the risks in processing criminal data and the repercussions of incorrect processing are higher.

6.8 Processing Children's Data[5]

6.8.1 In the UK, a child is considered to be anyone under the age of 18 (in line with the UN Convention on the Rights of the Child), and the GDPR explicitly states that children's personal data requires particular protection when you are collecting and processing their personal data because children may be less aware of the risks involved. Importantly children have the same rights as adults over their personal data, including the rights to access their personal data; request rectification; object to processing and have their personal data erased.

6.8.2 The GDPR contains provisions intended to enhance the protection of children's personal data and to ensure that children are addressed in a plain clear language that they can understand. Transparency and accountability are important where children's data is concerned and this is especially relevant when they are accessing online services. However, in all circumstances you need to carefully consider the level of protection you are giving that data.

6.8.3 If you process children's personal data then you should think about the need to protect them from the outset, and design your systems and processes with this in mind. Compliance with the data protection principles and in particular fairness should be central to all your processing of children's personal data. You need to have a lawful basis for processing a child's personal data. Consent is

[4] For further guidance regarding Schedule 1 of the DPA 2018 see Data Protection Act 2018 (legislation.gov.uk)

[5] Guidance as stipulated by the Information Commissioner's Office document 'Children and the GDPR'

one possible lawful basis for processing, but it is not the only option. Sometimes using an alternative basis is more appropriate and provides better protection for the child.

6.8.4 If you are relying on consent as your lawful basis for processing personal data when offering an online service (such as websites, apps, social media, search engines, online marketplaces and online content services such as on-demand music, gaming and video services and downloads) directly to a child, in the UK only children aged 13 or over are able to provide their own consent (as set out in the Data Protection Act, 2018). For children under this age you need to get consent from whoever holds parental responsibility for the child[6].

7 GDPR Safeguards (Protection for Participants)

7.1 General Safeguards

7.1.1 GDPR safeguards align with the principles of conducting ethical research and are protection for participants. They include:

- Not causing substantial damage or distress to research participants (this should be addressed in the ethics application);
- Not making decisions or measures that affect individuals on the basis of personal data (this is not likely to be relevant for the majority of research). There is an exception to this for ethically approved medical research;
- Respecting the principle of data minimisation, i.e. processing personal data that's adequate (sufficient to fulfil the research purpose), relevant and limited to what is necessary;
- Anonymising or pseudonymising, where possible;
- Understanding the importance of privacy, confidentiality and security (working to DMU codes of conduct, IT policies and technical standards will aid this);
- Meeting a separate public interest task for processing special categories of personal data over and above using '*task in the public interest'* as the lawful basis, such as peer review from a public funder or research ethics committee approval.

7.2 Individual Rights

7.2.1 The GDPR provides the following rights for individuals:

- **The right to be informed** - this covers some of the key transparency requirements of the GDPR. It is about providing individuals with clear and concise information about what you do with their personal data.
- **The right of access** - commonly referred to as subject access, which gives individuals the right to obtain a copy of their personal data as well as other supplementary information. It helps individuals to understand how and why you are using their data, and check you are doing it lawfully.
- **The right to rectification** - individuals have the right to have inaccurate personal data rectified. An individual may also be able to have incomplete personal data completed – although this will depend on the purposes for the processing. This right has close links to the accuracy principle. However, although you may have already taken steps to ensure that the personal data was accurate when you obtained it, this right imposes a specific obligation to reconsider the accuracy upon request.
- **The right to erasure** - individuals have the right to have personal data erased. This is also known as the 'right to be forgotten'. The right is not absolute and only applies in certain circumstances.

[6] For full guidance see ICO Children and the UK GDPR | ICO

- **The right to restrict processing** - individuals have the right to restrict the processing of their personal data in certain circumstances. This means that an individual can limit the way that an organisation uses their data. This is an alternative to requesting the erasure of their data. Individuals have the right to restrict the processing of their personal data where they have a particular reason for wanting the restriction. This may be because they have issues with the content of the information you hold or how you have processed their data. In most cases you will not be required to restrict an individual's personal data indefinitely, but will need to have the restriction in place for a certain period of time.
- **The right to data portability** - gives individuals the right to receive personal data they have provided to a controller in a structured, commonly used and machine-readable format. It also gives them the right to request that a controller transmits this data directly to another controller.
- **The right to object** - the GDPR gives individuals the right to object to the processing of their personal data. This effectively allows individuals to ask you to stop processing their personal data. The right to object only applies in certain circumstances. Whether it applies depends on your purposes for processing and your lawful basis for processing.
- **Rights in relation to automated decision making and profiling** - profiling is now specifically defined in the GDPR. Solely automated individual decision-making, including profiling with legal or similarly significant effects is restricted. There are three grounds for this type of processing that lift the restriction. Where one of these grounds applies, you must introduce additional safeguards to protect data subjects. These work in a similar way to existing rights under the 1998 Data Protection Act. The GDPR requires you to give individuals specific information about automated individual decision-making, including profiling. There are additional restrictions on using special category and children's personal data[7].

8 International Transfers of Data

8.1 There are different requirements relating to the transfer of personal data between countries and this has been complicated by the UK leaving the EU. This guidance reflects current practice as of 14 January 2021, but please note the situation is likely to change, one way or another, by the beginning of June 2021 at the latest.

8.2 Transfers from the UK to the EEA (and adequate countries): So long as the processing has a lawful basis, and adheres to the principles, data can be transferred from the UK to EEA, and countries deemed adequate by the EEA, without the need for additional safeguards.

8.3 Transfers from the UK to Third Countries: Most transfers of personal data to Third Countries (countries not deemed adequate by the UK government) can only take place if the transfer is covered by appropriate safeguards. It is recommended you always seek advice from the Information Governance Team if you are planning to transfer personal data to a third country. The main safeguards are as follows:

8.3.1 Binding Corporate Rules (BCRs):

- You can make a restricted transfer within an international organisation if both you and the receiver have signed up to approved BCRs. UK BCRs are approved by the Information Commissioner. BCRs are intended for use by multinational corporate groups, groups of undertakings or a group of enterprises engaged in a joint economic activity such as franchises, joint ventures or professional partnerships.

[7] Further full guidance is available at either Individual rights | ICO or guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf (publishing.service.gov.uk) (Page 52 Individual Rights)

8.3.2 Standard Contractual Clauses:

- You can make a restricted transfer if you and the receiver have entered into a contract incorporating standard data protection clauses recognised or issued in accordance with the UK data protection regime. These are known as 'standard contractual clauses' ('SCCs 'or 'model clauses').
- The SCCs contain contractual obligations on you (the data exporter) and the receiver (the data importer), and rights for the individuals whose personal data is transferred. Individuals can directly enforce those rights against the data importer and data exporter.

8.3.3 In addition to the above safeguards the Data Protection Act 2018, mirroring the GDPR, contains exceptions that can be used. Some examples of exceptions are listed below, but again it is recommended that you contact the Information Governance Team for guidance, as these are not as straightforward as they might appear.

- Explicit consent of the Data Subject (s)
- Transfer is necessary for the performance of a contract ➢ Vital Interests
- Make or defend a legal claim
- Compelling legitimate interests

8.4 Transfers from the EEA to the UK

8.4.1 Technically from the perspective of the EU the UK became a Third Country as of 1st January 2021 because we had left the EEA and we do not have an adequacy decision. As such transfers of data from the EEA to the UK would have required the same safeguards that UK transfers to Third Countries require, as above.

8.4.2 However, whilst the EU-UK Trade and Cooperation Agreement announced on the 24th December 2020 does not include an adequacy decision for the UK, it does define a further transition period of up to six months to enable the European Commission to complete its adequacy assessment of the UK's data protection laws. During this transition period personal data can continue to be exported from the EU to the UK without need for further safeguards.

8.4.3 The transition period begins on January 1st 2021 and will end either:

8.4.3.1 When an adequacy decision in relation to the UK is adopted by the European Commission;

8.4.3.2 Four months after the Specified Period begins (presumably 1st May), unless either the EU or the UK objects.

8.4.4 The EU may end the Specified Period early if the UK makes changes to its data protection legal framework.

8.4.5 The Information Commissioner's Office suggests it would be a sensible precaution for businesses to work with EU and EEA organisations who transfer personal data to them, to put in place alternative transfer mechanisms, to safeguard against any interruption to the free flow of EU to UK personal data, or in the event that an adequacy decision is not agreed before the end of the transition period.

9 Responsibilities for Data Governance

9.1 Privacy Notices

9.1.1 Our online privacy notice sets out information in relation to the privacy, rights and data protection guidelines/policies at DMU. The page advices how DMU uses personal information and how it is processed.

9.2 Key Contacts

9.2.1 The first point of contact for any data protection query should be your line manager. If the query needs further clarification or escalation, the line manager will contact the GDPR Lead for their directorate/faculty.

9.2.2 **Information Governance Team**

- Information Governance Team: dataprotection@dmu.ac.uk
- Information Governance Manager: Paul Starkey
- Information Governance Officer: Michael Davies
- IT Governance and Security Manager (located in ITMS): Danny Simon

9.2.3 There is also a **Data Protection Officer,** which is a statutory role, and which, due to its regulatory nature, sits independently outside of the Information Governance Team, but working alongside it on matters relating to data protection. The Data Protection Officer is responsible for overseeing data protection compliance for the university, with a particular role as the interface between supervisory authorities and the organisation.

- **Data Protection Officer:** David Parkes
- **Deputy Data Protection Officer:** Jon Hill
- **Email: dpo@dmu.ac.uk**

9.2.4 **GDPR Leads -** The role of a General Data Protection Regulation (GDPR) Lead is to take an active role in enabling DMU to be and remain GDPR compliant. The GDPR Leads coordinate individual business areas' GDPR audit responses, and act as the primary GDPR contact for staff within their domain. A list of current GDPR leads can be found here.

10 Data Protection Impact Assessments (DPIAs)

10.1 A Data Protection Assessment (DPIA) is a form of risk assessment. It is a way to help you identify and minimise the data protection risks of a research project, and identify the measures necessary to protect the privacy rights of your data subjects. The seven data protection principles set out in the GDPR form the basis of the DPIA and it can be used as a tool for demonstrating the GDPR principle of accountability and ensures privacy is by design and default.

10.2 A DPIA should be considered for any research project involving the processing of personal data and where it is likely to result in a high risk to the rights and freedoms of your data subjects, irrespective of any special category status. It is essential that you build data protection into your research project and by completing the DPIA at an early stage in the lifecycle of the research project, you are ensuring not only protection for your data subjects, but are maintaining transparency and accountability. Should you make any amendments to the research at a later date, you must re-visit the DPIA accordingly.

10.3 Having established your legal basis for processing the personal data, this will be recorded as part of the DPIA process alongside documentation in your ethics application.

10.4 Your DPIA must:

- describe the nature, scope, context and purposes of the processing;
- assess necessity, proportionality and compliance measures;
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.

10.5 A good DPIA helps you to evidence that:

- you have considered the risks related to your intended processing; and ➢ you have met your broader data protection obligations.

10.6 To assess the level of risk, a DPIA must consider both the likelihood and the severity of any impact on individuals.

10.7 A DPIA does not have to indicate that all risks have been eradicated. But it should help you document them and assess whether or not any remaining risks are justified.

10.8 A DPIA screening checklist and template are available on the DMU Intranet, along with our full DPIA guidance document Data Protection Impact Assessment (DPIA) (sharepoint.com)

11 Exemptions

11.1 There are some occasions where the Data Protection Act 2018 (DPA 2018) provides exemptions from certain GDPR provisions. If an exemption applies, you may not have to comply with all of the usual rights and obligations.

11.2 The exemptions in the DPA 2018 can relieve you of some of your obligations for such things as: ➢ The right to be informed;

- The right of access;
- Dealing with other individual rights; ➢ Reporting personal data breaches; and ➢ Complying with the principles.

11.3 Whether or not you can rely on an exemption generally depends on your purposes for processing personal data.

11.4 Some exemptions apply simply because you have a particular purpose. But others only apply to the extent that complying with the GDPR would:

- be likely to *prejudice* your purpose (e.g. have a damaging or detrimental effect on what you are doing); or
- *prevent* or *seriously impair* you from processing personal data in a way that is *required* or *necessary* for your purpose.

11.5 *Exemptions should not routinely be relied upon or applied in a blanket fashion*.

11.6 If an exemption does apply, sometimes you will be obliged to rely on it (for instance, if complying with GDPR would break another law), but sometimes you can choose whether or not to rely on it.

11.7 In line with the accountability principle, you should justify and document your reasons for relying on an exemption so you can demonstrate your compliance.

11.8 If you cannot identify an exemption that covers what you are doing with personal data, you must comply with the GDPR as normal.

11.9 There are various exemptions available (see ICO Guidance) however, for the purpose of this guidance, the most relevant are those included for research and statistics. Use of exemptions should always be reviewed by the Information Governance Team

12 Data Retention

12.1 Potential research participants should be made aware of your plans to store their data after the study has ended (usually during the consent process). This should include how long data will be kept, who will be responsible for it, what measures will be taken to protect confidentiality, and whether there are any intentions to share data with others, etc.

12.2 In line with the **storage limitation** principle of the GDPR, DMU has a Research Records Retention Policy that you should refer to regarding the creation, maintenance and disposal of research records. Although it applies primarily to funded projects, it is good practice to follow the principles outlined in relation to the conduct of any research. The GDPR sets out that:

- You must not keep personal data for longer than you need it.
- You need to think about – and be able to justify – how long you keep personal data. This will depend on your purposes for holding the data.
- You should periodically review the data you hold, and erase or anonymise it when you no longer need it.
- You must carefully consider any challenges to your retention of data. Individuals have a right to erasure if you no longer need the data.
- You can keep personal data for longer if you are only keeping it for public interest archiving, scientific or historical research, or statistical purposes.

12.3 However, you will need to be mindful that with NHS related research or funded research, data will need to retained in line with NHS/ funder requirements, for example the MRC have various levels of retention periods, depending on the type of study. So, it is important to refer to your research council or funder guidelines.

13 References and Resources

In formulating this document, the University has been informed by:

Information commissioner's Office

guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf (publishing.service.gov.uk)
Guide to the UK General Data Protection Regulation (UK GDPR) | ICO

British Psychological Society (BPS)

Data Protection Regulation: Guidance for Researchers | BPS

NHS Health Research Authority (HRA)

GDPR guidance - Health Research Authority (hra.nhs.uk)

Medical Research Council (MRC)

UK Data protection law and the common law of confidentiality - Research - Medical Research Council (ukri.org)

UK Research and Innovation (UKRI)

https://www.ukri.org/about-us/policies-standards-and-data/gdpr-and-research-an-overview-for-researchers/

Other Resources

MRC – Retention Framework for Research Data and Records
Background and scope (ukri.org)

14 Document Version Control & Update Information

Version	Date	Updates	Changes made by
0.1	21.01.2021	Final Version	S.Fowler (Research Services)
0.2	19.04.2021	Minor changes following Brexit to change from EU to UK	S.Fowler (Research Services)