Research Services Directorate

.

UK GENERAL DATA PROTECTION REGULATION (UK GDPR) GUIDANCE FOR RESEARCHERS

Created and Modified:	21 January 2021
Last Updated	05 January 23
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 UKGDPR?

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, 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.

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.

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.

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.

For the GDPR to apply, you must be processing personal data (as defined below).

The GDPR recognises 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

Below are some of the most important and common definitions that relate to the GDPR. This

vi. Processed in a manner that ensures appropriate security of the personal data (confidentiality and integrity);
vii. Accountability.

4 Lawful Bases for Processing

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

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).

The requirement to have a lawful basis

For full relevant provisions in Article 6 see https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

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:

> 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 the task 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.
>
> 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. In addition, it can be problematic to change your lawful basis after the processing has begun.

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'.

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

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

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

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.

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.

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

6.4 Pseudonymised Data

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)

X. 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.

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.

Non-commercial research conducted at DMU is done in the public interest, therefore, where our research involves special category data, we will usually rely on 'processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes' 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

This means you must either:

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

Even if you have a condition, as per Article 9 (2) for processing offence data, you can only keep a comprehensive register of criminal convictions 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.

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.

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]

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.

The GDPR contains provisions intended to en Ə □ = = Æ ő ta

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[3]

Note that if you are offering such services to children within the EU you should consult with the Information Governance team as the age restriction will vary between countries.

7 GDPR Safeguards (Protection for Participants)

7.1 General Safeguards

GDPR safeguards align with the principles of conducting ethical research and are protection for

- 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;
- 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

8.1 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.

8.2 Standard Contractual Clauses/International Data Transfer Agreements

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.

From 2022 the ICO have introduced International Data Transfer Agreements and Addendum templates

9.2 Key Contacts

Your DPIA must:

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

A good DPIA helps you to evidence that:

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

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

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.

A DPIA screening checklist and template are available on the DMU Intranet, along with our full DPIA

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

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

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

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.

In line with the storage limitation principle of the GDPR, DMU has a 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:

- ü You must not keep personal data for longer than you need it.
- ü 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.
- ü You should periodically review the data you hold, and erase or anonymise it when you no longer need it.
- ü You must carefully consider any challenges to your retention of data. Individuals have a right to erasure if you no longer need the data.
- ü You can keep personal data for longer if you are only keeping it for public interest archiving, scientific or historical research, or statistical purposes.

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.

Questions related to Records Management should always be directed towards the university's Records Manager Jenny Moran

13 References and Resources

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

Information Commissioner's Office
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)
UK Research and Innovation (UKRI)