Data Protection Standard for Research (incorporating GDPR)

Contents

1 Introduction

The aim of this Standard is to define the framework within which personal data processed for research purposes must be conducted at the University of the West of England, Bristol (UWE) to comply with relevant data protection requirements. Compliance with this Standard relates to compliance with data protection legislation, but there may be additional measures necessary to ensure that research also complies with good ethical practice. This Standard is therefore **not intended to replace the ethical approval process, or address ethical issues** as there will be occasions where something may be permitted by law, but will not necessarily be granted ethical approval. For further information about applying for ethical approval at UWE please see:
http://www1.uwe.ac.uk/research/researchethics.aspx

NB: Sections 4-10 below set out requirements which research projects must consider adding to their project design to demonstrate the position/action on data management by default. This information can be added to the ethical application form and data management plan to demonstrate the project's data protection compliance.

2 Definitions

For the purpose of this Standard the following definitions apply:

2.1 UWE

The University of the West of England, Bristol.

2.2 Research

Research is defined for the Research Excellence Framework and by UWE as including the following:

> '1. For the purposes of the REF, research is defined as a process of investigation leading to new insights, effectively shared.
>
> 2. It includes work of direct relevance to the needs of commerce, industry, and to the public and voluntary sectors; scholarship[1]; the invention and generation of ideas, images, performances, artefacts including design, where these lead to new or substantially improved insights; and the use of existing knowledge in experimental development to produce new or substantially improved materials, devices, products and processes, including design and construction. It excludes routine testing and routine analysis of materials, components and processes such as for the maintenance of national standards, as distinct from the development of new analytical techniques. It also excludes the development of teaching materials that do not embody original research.

[1] Scholarship for the REF is defined as the creation, development and maintenance of the intellectual infrastructure of subjects and disciplines, in forms such as dictionaries, scholarly editions, catalogues and contributions to major research databases

3. It includes research that is published, disseminated or made publicly available in the form of assessable research outputs, and confidential reports (as defined at paragraph 115 in Part 3, Section 2).'[2]

2.3 Data Protection Legislation

This means the European Directives 95/46/EC and 2002/58/EC (as amended by Directive 2009/139/EC) and any legislation and/or regulation implementing or made pursuant to them including but not limited to the Data Protection Acts 1998 and 2018, and legislation which amends, replaces, re-enacts or consolidates any of them including but not limited to the General Data Protection Regulation, EU 2016/679, and including, where applicable, the guidance and codes of practice issued by supervisory authorities (including the Information Commissioner's Office).

2.4 Data Controller

'Data controller' refers to the person or organisation determining the purposes for and manner in which any personal data are to be processed.

UWE's Data Protection Officer supports UWE in ensuring compliance with data protection legislation in relation to all of its activities. The Data Protection Office is a point of contact for data protection queries and can be contacted by email at: dataprotection@uwe.ac.uk.

In some instances UWE will be joint data controller with other organisations or individuals either jointly determining the purposes and manner of data processing or independently doing so. See section 5.2 below.

2.5 Data Processor

The data processor is the person or organisation responsible for processing personal data on behalf of the data controller.

Examples of data processors processing personal data on behalf of UWE include transcription service providers and public research partners.

2.6 Data Subject

The data subject means the identified or identifiable living individual to whom the personal data relates.

2.7 Personal Data

Personal data means any information that can be attributed to an identifiable living individual.

[2] HEFCE (2011) *Assessment framework and guidance on submissions*, REF 02.2011, July 2011, Annexe C, p.48. Online at: https://www.ref.ac.uk/2014/media/ref/content/pub/assessmentframeworkandguidanceonsubmissions/GOS%20including%20addendum.pdf

2.8 Special Category Data

Special category data is personal data which the GDPR and/or other legislation states is more sensitive than simply personal data. It has more restrictions upon processing and needs more protection than personal data.

The following types of personal information are defined as special categories: data relating to health (physical and mental), ethnicity, sexual orientation, sex life, trade union membership, biometric or genetic data, and political, philosophical and religious opinions/beliefs. Details of criminal offences and convictions and related security measures must also be afforded similar treatment.

2.9 Anonymisation of Data

Anonymisation of data is the process of turning data into a form which cannot identify individuals, including the data subject, and where re-identification of those individuals cannot take place. Anonymised data is not subject to data protection requirements and can therefore be used and re-used without further permissions from the original data subject. Thus anonyised datasets made suitable for the UK Data Archive, or the results of data analysis which are presented at Conferences or in peer reviewed journals are not subject to data protection restrictions.

2.10 Pseudonymisation of Data

Pseudonymisation is the process of de-identifying individuals whilst leaving a means of re-identifying them. This is most commonly used in research during the period when research participants could ask to be withdrawn from a study, rendering it necessary for the researcher to have a means of re-identification.

Pseudonymmised data must still comply with data protection requirements as individuals can still be re-identified.

Care should also be taken so that the research methodology does not facilitate unintentional re-identification of individuals. This could occur, for example, by using a very small sample of participants from a cohort where individuals would be easily identifiable, or where a de-identified dataset could be linked with other published data which would re-identify individuals.

3 Scope

This Standard applies to **all instances where personal data is processed for the purpose of research** (as defined in the introduction). It includes (but is not limited to):

All research (whether externally or internally funded, including staff research, PGR research, PGT and UG research, including research conducted either solely by the University or in collaboration with a third party.

More detailed guidance will follow in due course for supervisors of PG and UG research. It is important that supervisors ensure students are aware of the legislation requirements relevant to their research. Supervisors are responsible for the conduct of student research projects

4 The Principle of 'data protection by design and default'[3]

This section sets out the principle that data protection must be designed into projects. It refers specifically to the rules under Article 25 of the GDPR whereby the data controller must implement appropriate technical and organisational measures for ensuring that, **by default**, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.

This means that GDPR and the associated data protection legislation referred to in paragraph 2.3 above must be considered at all stages of the research lifecycle of the project. This includes all stages of the resaerch involving the collection, transportation, translation into different forms, storage, use, disposal, sharing, archiving and any other form of processing of personal data.

4.1 Data Protection Impact Assessment (DPIA)

The purpose of a Data Protection Impact Assessment (DPIA) is to assess data risks. Areas of research likely to require a DPIA are those where the subjects are vulnerable including (but not limited to) children or people with learning disabilities), and special categories of personal data including large volume data or administrative data. More detailed information about vulnerable subjects and special categories is available at: https://intranet.uwe.ac.uk/tasks-guides/Guide/data-protection

4.2 Data Minimisation

An important principle of GDPR is data minimisation. This means that at all times, personal data collection, storage and use must be kept at the minimum level to allow the research to take place. In some instances, it will be possible not to collect any identifiable information, including even IP address.

Researchers must not collect more personal data than is needed, and personal data must only be kept for as long as necessary. **This generally means that once data has been anonymised, the personal data must be securely destroyed**.

Researchers must take an active decision in this respect, collecting only that personal data that is necessary and retaining it only for as long as necessary. Researchers should always remain in a position to justify a decision to retain personal data.

further guidance on data destruction standards for consent forms to follow

4.3 Technical and Organisational Measures

The UWE Research Data Policy specifies that research which involves research data **must have a Research Data Management Plan (RDMP)**. This must specify how research data will be handled

[3] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-*protection*-by-design-and-default/ and UWE research data management policy: http://www1.uwe.ac.uk/research/researchgovernance/resourcesforresearchers/researchdatamanagement.aspx

throughout its lifecourse, including collection, transportation, storage, archiving, sharing and disposal. In order to be GDPR compliant, the RDMP must include records of how the data will be processed

further guidance and an updated RDMP template will be made available in due course.

5 Data Processing Agreements and/or Data Sharing Agreements

5.1 Data Processing Agreements

Personal data cannot be processed by a third party[4] unless a third party **Data Processing Agreement** has been approved and signed by an apporoved signatory on behalf of the University and the third party Data Processor. More detailed guidance is available at:

https://intranet.uwe.ac.uk/tasks-guides/Guide/data-protection#part4

If you need a Data Processing Agreement or any associated advice, please contact the Data Protection Office at dataprotection@uwe.ac.uk.

5.2 Data Sharing Agreements

Where there is more than one data controller it may be necessary to agree a **Data Sharing Agreement** between the respective parties. If you need a Data Sharing Agreement please contact the Data Protection Office at dataprotection@uwe.ac.uk.

6 Data Transfers outside the European Economic Area (EEA)

Extra safeguards will be required where personal data is transferred or processed outside the European Economic Area (EEA). Please note that international transfers of personal data includes use of software such as survey tools where the data is stored on a server outside the EEA.

Please note the only survey tool authorised by the University is Qualtrics. Other surveys may use servers outside the EEA and are therefore not compliant. If you want to use any online survey other than Qualtrics, please contact the Data Protection Office (dataprotection@uwe.ac.uk)

Transfers of personal data outside of the EEA is **prohibited** unless one of the following exceptions applies. Please contact the Data Protection Office for confirmation you can rely on one or more of these exceptions:

- The country or territory has received an adequacy ruling from the European Commission
- Transfer is subject to standard contractual clauses approved by the European Commission
- Transfer is to a US organisation which has certified itself to the EU/US Privacy Shield
- Binding corporate rules exist within transnational organisations
- Data subject has given explicit consent for transfer after being informed of any risks that the transfer may pose to their rights and freedoms

[4] Meaning anyone outside the University, including other universities, health care trusts, companies, charitable organisations or individuals.

- Another specific derogation from this prohibition applies.

7 Retention and disposal of data

The principle of data minimisation should apply to all stages of project design and implementation. The data retention period for all types of data must be justified and agreed to in the participant consent form. Data archiving of any personal data must be in line with the consent given by the participant.

Disposal of data must be by secure deletion from devices, secure shredding of paper documents or other secure method of destruction.

8 Data subject rights

8.1 Data Privacy Notice

A Privacy Notice which complies with GDPR requirements must be provided to participants and/or data subjects prior to collecting/using data. Guidance is available at:
http://www1.uwe.ac.uk/about/corporateinformation/datamanagement/privacynotices.aspx

8.2 Informed Consent

Informed consent from the data subject, or the data controller must always be in place for the use of personal data, and data should only be processed in accordance with the terms of the consent. Informed consent from research participants must be obtained, recorded and stored securely in accordance with the University's Information Security Policy, available at:
http://www1.uwe.ac.uk/its/informationsecuritytoolkit/policies/informationsecuritypolicy.aspx

9 Research Exemptions

Similarly to previous data protection legislation, GDPR recognises the importance of enabling research. This is reflected in some research exemptions from GDPR's provisions. However these exemptions can **only** be applied if the provisions of this Standard are met, and the exemptions are **necessary to fulfil the purposes of the research**. Exemptions relevant to research include (but are not limited to):

- Some data subject rights are limited. For example the right to erasure of personal data where this would compromise the research;
- Data may be retained for longer periods of time exempt from storage limitation principle;
- Research data may be exempt from the purpose limitation principle as data collected for one purpose can be used for research purposes if certain conditions are met.

Please note that these exemptions do not exempt the researcher from following the University's ethical approval process.

10 Ethical approval

Ethical approval **MUST** be granted by UWE's Faculty or University Research Ethics Committee in respect of research and/or evaluations involving the collection of personal data, or the use of exisiting personal data, undertaken either by UWE (including its students and staff), or external third parties undertaking their research at UWE or using UWE employees or students as participants. Data collection elements of projects must not start **until ethical approval has been granted by the University**. UWE's approval must be obtained **in addition to** any necessary external ethical approval. UWE's research ethics policies, guidance and application forms are available at: http://www1.uwe.ac.uk/research/researchethics.aspx

v.1.1 Authors: Steve Dinning and Ros Rouse