Data Protection guidance note from the Information & Data Compliance Team for researchers applying for Research Ethics approval

The below guidance is intended to provide clarity on commonly used terms relating to GDPR and give researchers more information about how to complete the questions in section 8 of the Ethics Application form. This guidance should be tailored to suit individual projects. It should help researchers to consider the safeguards that need to be put in place to ensure compliance with Data Protection Principles and avoid accidental disclosure of personal information.

Data Flow Map

A template data flow map has been provided to accompany the ethics application form to help determine who the data controllers and processors are in the project. Researchers do not have to use this template but can use this as a guide to design their own. The complexity of the data flow map will depend on the project, the number of collaborators/third parties and data processing activities.

A **Data Controller** is the party which determines the purposes and means of processing personal data. This means, the party who has control over what information is collected and how this will be used. It is possible for there to be more than one controller for each process, each with their own purpose.

A **Data Processor** is the party who processes personal data on behalf of the Data Controller. This is an individual or organisation who is processing data in accordance with someone else's (the controller's) instructions. *Please refer to the ICO's guidance if you are in any doubt.*

The Data Flow Map should:

- document what happens to the data from the point of collection to the point of deletion (or review to decide if the data should be retained or deleted);
- account for the storage/processing of data within any third parties and also any cloud services (i.e. sharing or transferring the data for randomisation, analysis, transcription or other research activities);
- include details of how long information is retained at the various stages and who may be granted access to the data;
- consider arrangements for long term storage and archiving of the data.

Further guidance and support with regards to managing research data is available from the Library.

Questions 8.2 and 8.3: These questions ask for information relating to the type of data that will be collected and the justification for collecting this (e.g. research aims)

Please find below guidance for the following question: '*What measures are being implemented to reduce or eliminate the risk to these participants' data for the duration of the period that their personal data is collected and stored?*'

This question is looking to determine what measures researchers are putting in place to reduce the risk to data at various stages such as:

- restricted access to the data
- password protection of systems
- ensuring that third party systems have been through the Information Security workbook

- data minimisation at the appropriate stage so only the required data sets are being held
- anonymising/pseudonymising data
- enforcing retention periods – when and how are copies of the data deleted

See below guidance on Question 8.10 for more detailed information on these points

Special Category Data – Additional Safeguards

The processing of Special Category Data requires that an additional processing condition is satisfied in addition to the usual lawful basis for processing. More guidance can be found here: **https://warwick.ac.uk/services/idc/gdpr/keyterms**

Question 8.7: Data Sharing

Data sharing refers to the disclosure of data to third party organisations, or the sharing of data between different parts of the same organisation.

Data sharing can be in many forms including: a reciprocal exchange of data; one or more organisations providing data to a third party or parties; several organisations pooling information and making it available to each other or different parts of the same organisation making data available to each other.

Where personal data will be shared with a third party, including external collaborators, external transcription services and cloud service providers, there must be an appropriate data sharing agreement in place before any data transfer takes place. This must be signed off on behalf of the University and not the researcher themselves. Please contact Research & Impact Services (R&IS) for information on preparing data sharing agreements.

Where data will be shared during or after the research process, whether this is with a supervisor, internal or external collaborator or another authorised individual, researchers should ensure they are using the Warwick email server and not personal accounts e.g. gmail or Hotmail. Files.Warwick is a secure tool researchers can use to store and share their research files securely, accessing them via a web browser. This is particularly useful when there is a need to share a file that is greater than the University's 10 MB limit for email attachments. These can also be shared with external individuals via a web browser.

Question 8.9: Sharing Data outside the UK

The University works with many organisations in Countries and territories which fall outside the European Economic Area (EEA). In order for us to continue to share personal data with organisations in these regions, the GDPR has additional requirements that researchers need to comply with when sharing data. Please contact researchgovernance@warwick.ac.uk for further guidance before making any data transfers outside the EEA for research purposes.

Researchers also need to be aware that using international cloud-based services and international software/data collection methods may involve a transfer of personal data outside the EEA. Signing up to such a service in your role as a member of University staff may be binding the University (and not just yourself) to the service's contractual terms, which may not fully comply with the GDPR and therefore put the University at risk of a data breach. The risk is even greater where the data being shared is considered special category personal data or confidential information.

Question 8.10 - Describe compliance and proportionality measures in place to satisfy the requirements of the Data Protection Act 2018 and the GDPR.

e.g. how will you ensure: fairness and transparency to research participants, data quality, data minimisation (only collect data which is necessary for the purpose(s) of the study), purpose limitation (no further processing of the data for purposes incompatible to those for which it was collected), de-identification of the data as soon as possible, appropriate technical and organisational measures in place to avoid unauthorised access and accidental loss or damage to data etc.

This question addresses Article 5 of the GDPR: principles relating to processing of personal data. Any breach of this provision could result in substantial fines for the University and sanctions for the individual themselves. This question is looking for researchers to consider how they will address each data protection principle to ensure they will be compliant.

There must be an established and documented lawful basis for processing personal data, for research, this is 'task in the public interest'. For personal data to be used for research, researchers must ensure they employ safeguards including organisational and technical measures to prevent accidental disclosure of personal data to unauthorised individuals and to ensure no harm or distress is caused to individuals. These are as follows:

1. **Data minimisation** should be applied to the research project and the following 3 things should be considered:

    1.1 Only the amount of data required for the study should be collected, from the minimum number of participants (researchers should justify this with a sample size calculation to evidence this is appropriate to the methodology, statistical analyses required and research outcomes/objectives);

    1.2 The minimum amount of personal data should be collected from each participant, again justified by the research design;

    1.3 The degree of sensitivity of the personal data collected should also be minimised - if special category (sensitive) data is not required to achieve the outcomes of the project, it should not be collected. E.g. is knowing a participant's religious beliefs or ethnicity relevant to the research question? If not, it shouldn't be collected.

2. **Pseudonymisation/anonymisation** - data should be anonymised/pseudonymised as soon as possible. Pseudonymisation involves the removal of direct or common identifiers from the data set, which are then replaced with a number or a code so data can be continually collected about an individual without recording their identity. For pseudonymised data to be secure, the key to re-identifying individuals from the data must be stored separately and securely to the research data. Access to this key should be restricted. If you no longer need to be able to identify a participant, the key should be destroyed. Data is only considered anonymous when there is no possible way to identify an individual either directly or indirectly from the data set.

3. **Transparency -** the data must be obtained openly and honestly and without any misleading intentions. Details of what personal data will be collected and how this will be processed (intended use), shared and stored should be explicit in the Participant Information Leaflet (PIL). The PIL needs to be specific to the research project but the PIL template provided will help to ensure transparency requirements are met. Participants should also be made aware of when their personal data will be deleted.

4. **Fairness** - data should only be handled in a manner that the individual would expect to be deemed 'fair'. The use of the data should be made clear to participants at the outset, as above.

5. **Technical measures** for example password protection, encryption, restricted access, locked filing cabinets should be applied. All researchers should use University managed devices (laptops/PCs/phones) when processing personal data for research. Research data should be stored on University secure servers and for no longer than is entirely necessary. Any hard copy data e.g. consent forms should be stored in accordance with the University's information handling procedure: https://warwick.ac.uk/services/idc/informationsecurity/handling

6. **Data sharing –** see above guidance for question 8.7. Confirm that arrangements have been made to ensure that all data sharing processes are GDPR compliant.

7. **Data sharing agreements** – see above guidance for questions 8.7 and 8.9 and confirm that any required data sharing agreements have been/will be put in place.

8. **Information Security** - information security workbooks should be completed where third party apps/services will be processing personal data on behalf of the University in a research project. For a list of University approved services for research e.g. transcription services, survey tools, please see the Information & Data Security webpage (please note, this is an ongoing project which the IDC team are continuing to add to).

9. **Using data for new purposes**: reuse of data for future research is not always known at the outset but if you are planning for the data to be made available for use in future research, this should be made clear to participants in the Participant Information Leaflet (PIL) and the consent form. Please note any future use of the data for research will require a new research ethics application to the relevant committee.